UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

"Propuesta de un sistema de comunicación para interconectar las sedes, INSFOP y UNICAM en los departamentos de Estelí y Madriz respectivamente."

Autores:

Br. Canales González Hardy Ariel Carnet: 2009-31662

Br. Moreno Viachica Noel Eduardo Carnet: 2009-31835

Br. Pastrana Ventura David Josué Carnet: 2009-31735

Tutor: MSc. Ing. Fernando Flores Guido

Octubre 2014

Managua, Nicaragua

DEDICATORIA

Hardy Canales:

Principalmente a mi Madre Idania quien me ha apoyado incondicionalmente durante el transcurso de mi vida, a mis hermanos Carlos y Grace quienes me han brindado mucho soporte, a mi Padre Carlos que en paz descanse, a nuestro tutor maestro y amigo Fernando Flores quien nos dotó con esmero de sus conocimientos, a Karina y Noel quienes demostraron ser excelentes amigos, a los compañeros, maestros y conocidos que directa o indirectamente ayudaron con la elaboración de este documento y sobre todo a Dios quien nos otorgó la vida y espíritu que nos permitió llegar hasta aquí.

Noel Moreno:

Le agradezco principalmente a Dios que me permitió dar este gran paso, a mis padres que apoyaron en todo momento y me ayudaron hasta el final, al profesor Fernando que nos enseñó, nos formó como buenos profesionales, y a todos los maestros que tuve que de alguna manera siempre nos enseñaron y nos transmitieron su conocimiento. También a Hardy, David y Sergio que de alguna manera siempre aportaron cosas positivas y entusiasmo para salir adelante.

David Pastrana:

Agradezco principalmente al Dios Padre Omnipotente, quien guía mis pasos, que está y ha estado conmigo en los momentos más difíciles.

Agradezco a mi Madre Marbelly Ventura, en primer lugar por darme la vida, cuidarme de niño y estar presente en los momentos más importantes de mi vida y que con mucho esfuerzo y amor me ha dado la oportunidad de realizar mis estudios primarios, secundarios y universitarios. Agradezco a mi Padre Ruddy Pastrana por cultivar en mí el amor al estudio y al trabajo, a todos mis maestros y maestras.

RESUMEN

El presente documento, tiene como objeto brindar una propuesta de diseño de un sistema de comunicación que permita interconectar 2 sedes de la institución INSFOP (Instituto de Formación Permanente) en Estelí, con una sede afiliada llamada UNICAM (Universidad Campesina) en Somoto, Madriz, con el fin de brindar servicio de voz, video y datos en general. El mismo ha sido elaborado en función de la necesidad existente, sobre los efectos que presienten las instituciones debido a los retardos a la hora de emitir orientaciones, que de una u otra manera les está conllevando a realizar sus planes operativos a un ritmo muy lento, lo que afecta directamente sus planes estratégicos y por ende a la misión de las instituciones.

Al dar inicio a este proyecto se realizó un estudio para determinar las condiciones y necesidades más sentidas por las instituciones con respecto a este problema, se obtuvieron datos necesarios para la elaboración de una propuestas; se descubrieron diferentes aspectos, dentro de los más importantes están las ubicaciones geográficas y los recursos con que contaban ambas instituciones para determinar qué tipo de tecnología sería la más adecuada para este proyecto, con la ayuda de nuestro tutor y demás ingenieros que operan y administran sistemas de telecomunicaciones en nuestro país, se consideró que lo más apropiado sería la ubicación de un sistema de radio enlace punto a punto para interconectar la sede rural y urbana de INSFOP ambas ubicadas en la Ciudad de Estelí, así como también un sistema de VPN que interconecte INSFOP central con su filial UNICAM ubicada en Somoto, Madriz, y sumado ello un sistema PBX utilizando un servidor dedicado con Asterisk, para que se realicen todas las comunicaciones de llamada (VoIP) utilizando las estructura de red antes diseñada. Esta propuesta se realizó teniendo presente la expansión futura de los servicios. Se hará uso del Software CISCO Packet Tracer para demostrar el funcionamiento y la disponibilidad de toda la infraestructura propuesta. Así mismo se realizó un presupuesto lo más económico posible que contiene los equipos necesarios para la realización de nuestra propuesta.

ÍNDICE

CONTENIDO **PAGINA**

INDICE DE FIGURAS

INTRODUCCIÓN

La comunicación vocal es una de las partes más importantes en el desarrollo humano. La necesidad del hombre de comunicarse a grandes distancias ha influido en su desarrollo a todos los niveles y en todas las épocas, desde los niveles personales, hasta niveles económicos, desde desarrollos locales hasta desarrollos nacionales o continentales, por ende el progreso tecnológico es un proceso inherente a las empresas; así como también a los servicios y aplicaciones telefónicas con las que interactúan dichas entidades con el fin de tener eficiencia de comunicación interna y externa, de esta manera se está proporcionando automatizaciones a ciertos procesos que facilitan la comunicación y aseguran que ésta sea versátil y sencilla, asimismo se provee integridad de los datos que fluyen en la red con el fin de que siempre sean íntegros.

Han surgido tecnologías que han modernizado la comunicación actual al menor costo posible, por tanto las empresas como las instituciones necesitan mejorar sus comunicaciones e INSFOP es una de estas, por lo se planteara una propuesta tecnológica eficiente que permita utilizar un nuevo servicio, en el cual se encuentran involucrados las diferentes sedes abocadas a INSFOP (Instituto de Formación Permanente) que es una organización que se dedica a llevar a cabo el desarrollo de diversos proyectos que benefician a muchas familias rurales lo cual permite contribuir al desarrollo humano, social y económico con enfoque de sostenibilidad. Con esto se pretende que la comunicación sea más versátil y ligera implantando consigo un uso más eficiente de las horas productivas e incrementado así sus prestaciones.

Esta propuesta consiste en atacar sus debilidades, por medio de un diseño bien estructurado que garantice una mejor comunicación entre las distintas áreas y filiales que conforman esta institución, y asegurar que una implementación del proyecto será de gran beneficio para las distintas partes involucradas en los proyectos que se llevan a cabo por la institución.

OBJETIVOS

OBJETIVO GENERAL

- ✓ Elaborar una propuesta de un sistema de comunicación para interconectar las sedes INSFOP y UNICAM en los departamentos de Estelí y Madriz respectivamente con el fin de brindar servicio de voz, video y datos en general.

OBJETIVOS ESPECÍFICOS

- ✓ Realizar un diagnóstico de la infraestructura de red de las instituciones, para conocer las características del equipamiento existente.
- ✓ Presentar un diseño de radio enlace punto a punto para interconectar la sede rural con la urbana de Estelí, ambas propias a INSFOP.
- ✓ Diseñar una VPN que interconecte INSFOP central con su filial UNICAM ubicada en Madriz.
- ✓ Proponer un servidor PBX virtual por medio del cual se realicen todas las comunicaciones (VoIP) utilizando la estructura de red que se diseñara.
- ✓ Determinar los costos del proyecto para dar a conocer la inversión requerida.

PLANTEAMIENTO DEL PROBLEMA

Actualmente, las comunicaciones telefónicas en el Instituto de Formación Permanente (INSFOP) y sus sedes, son limitadas; existen pocas líneas telefónicas y extensiones telefónicas internas; La central telefónica ubicada en la sede de la parte urbana de la ciudad de Estelí, no es extensible, es decir, no existe la posibilidad de crear extensiones telefónicas adicionales por falta de interfaces. Debido a la escasez de extensiones telefónicas, los usuarios de la institución se ven la necesidad de compartir los dispositivos de comunicación (teléfonos) para realizar sus tareas diarias. Otro aspecto que se pudo notar durante el diagnóstico, es que las conexiones de los teléfonos tienen mucho tiempo de existir y gran parte de estas ya son obsoletas. Esta situación dificulta el acceso por parte de los usuarios a los servicios de comunicación para compartir información.

La institución INSFOP tiene la necesidad de interconectarse con su sede rural ,que se ubica a unos 10 kilómetros de la ciudad de Estelí, en la cual todavía no hay presencia de proveedores de servicios de Telecomunicaciones (TSP) y por ende tienen muchas dificultades de comunicación, entre los problemas de mayor repercusión está la necesidad de movilizarse hacia la sede rural para realizar múltiples capacitaciones, proveer información e instruir las técnicas apropiadas para impartir cada capacitación de índole social, lo que incurre a múltiples gastos operativos.

Existe otro organismo afiliado a INSFOP situado en el departamento de Madriz, UNICAM (Universidad del Campesino), el cual también necesita interconectarse para compartirse cierta información, de manera que ambas Instituciones trabajen como una contraparte más sólida y más cerca una de la otra, y que el impacto social que estas tengan, sea mayor para el bienestar de las personas beneficiadas por los proyectos que estas impulsan, cabe resaltar que ambas instituciones tienen mucha presencia en gran parte del norte y centro del país.

JUSTIFICACION

El Instituto de Formación Permanente es una organización ubicada en el departamento de Estelí, que actualmente se encuentra en segundo lugar en generar ingresos al país, esta institución es reconocida en el ámbito nacional, con capacidad de liderazgo en las regiones norte del país dedicada a la formación y capacitación de personas sin acceso a la información en contextos agrícolas, culturales y de múltiples índoles que le permite contribuir al desarrollo humano, social y económico con enfoque de sostenibilidad; tiene un rol protagónico en las redes de trabajo con entidades afines, estado, gobiernos locales y sociedad civil, para movilizar y optimizar recursos monetarios, materiales y humanos hacia los grupos metas. Ésta Institución, sin fines de lucro, tiene dificultades al asumir el presupuesto para cubrir todos sus gastos, por ello el interés primordial es **PROPONER** una solución asequible para que puedan mejorar su productividad y consigo contribuir a la razón social de ésta Institución nicaragüense.

Como ingenieros en Telecomunicaciones se planteará la propuesta de un radioenlace para interconectar las sedes (Rural y Urbana de INSFOP en Estelí), el radioenlace además de interconectar ambas sedes de INSFOP proporcionara conexión a internet evitando así la necesidad de contratar un servicio de algún ISP(Proveedor de Servicios de Internet); Una red convergente basada en una VPN(Red Privada Virtual) que conecte a las sedes de INSFOP ubicadas en Estelí con su filial UNICAM en Madriz , una central telefónica basada en un Servidor de Telefonía por IP, que les permita repartir un mayor número de extensiones entre las sedes sin incurrir a gastos de teléfonos físicos ya que dichas extensiones se pueden administrar y operadas por Software basados en el Sistema Operativo Windows, la propuesta consiste más que todo en solucionar el problema de comunicación de estas instituciones, ya que corresponde a nuestra área resolver problemas de esta temática, por ende se aplicarán los conocimientos ilustrados por los docentes de la Universidad Nacional de Ingeniería y las experiencias obtenidas en las prácticas de laboratorios realizados en la Facultad de Electrónica y Computación (FEC).

CAPÍTULO I

1.1- DIAGNOSTICO

1.1.1 INSFOP ESTELÍ

Una vez hecho el levantamiento en la sede central INSFOP Estelí se cuenta con 2 líneas telefónicas análogas, tiene un ancho de banda de 5 MB, cabe mencionar que la infraestructura de red actual que ellos tienen interconectadas solo 12 pc donde el total de máquinas que ellos tiene en uso de la sede son 49 computadoras marca hp con 1GB de memoria RAM, un procesador Dual Core 2.5GHz características suficientes para instalar la tecnología propuesta. Producto de una donación INSFOP cuenta con 5 switch 3400 24-TS marca cisco el cual ya lo cual ya 3 de ellos ya se encuentran en uso 2 de ellos en cada sede de la institución.

Luego en la sede Rural de Estelí (Ubicada en San Roque)una vez realizado el estudio, no se cuenta con ninguna línea telefónica ni servicio de internet tienen 5 computadoras pero la cual no las tienen interconectadas debido a que no le encuentran sentido interconectarlas sin ninguna funcionalidad, se detectó la necesidad de utilizar un enlace de microondas, debido a que se encuentran a 10 kilómetros al sur-oeste de Estelí, como se explicó con anterioridad, no existe un proveedor de servicios de telecomunicaciones (TSP), lo que dificulta la comunicación con su central ubicada en el barrio El Calvario y por consiguiente a la sede ubicada en la ciudad de Madriz(UNICAM), Esto dificulta en gran manera a las operaciones de la institución, la cual se ve obligada a incurrir a gastos varios, para cumplir con sus programas, que muchas veces no se hacen en tiempo y forma.

Una vez que se tomó la decisión, era necesario saber si la ubicación y condiciones de ambas sedes, permitirían implementar esta tecnología, por lo que se recurrió a realizar un análisis del terreno (Site Survey), en el cual destacan los siguientes -aspectos:

-Con respecto al acceso en la sede rural está ubicada a 10 km de distancia de la oficina central y a aproximadamente 30 minutos en vehículo, el camino no está en buenas condiciones pero se puede acceder en vehículo para realizar la instalación de las antenas.

-La localización geográfica la obtuvimos con la ayuda de un Sistema de Posición Global (GPS), el cual nos arrojó las siguientes coordenadas:

En la sucursal de INSFOP que se ubica en la comunidad de San Roque, se obtuvo las coordenadas: **13º 4´ 32.4" N**, **86º 23´ 47.3" W**, y en la sucursal INSFOP ubicada en el barrio EL Calvario en la parte urbana de la ciudad de Estelí: **13º 4´29.3" N**, **86º 21´19.8" W**. Las condiciones ambientales, son favorable con un clima bastante cálido. Los equipos pueden instalarse fácilmente y ser integrados a red existente, debido a su arquitectura basada en IP pura.

-En ambas sedes amerita estructuras de torres livianas con uso de vientos para su soporte; En el cálculo de altura de antenas se verá la cantidad de tramos que se necesitaran para cada sede. Es importante mencionar que se observó que en los techos de las estructuras se puede hacer la instalación, lo que compensaría altura y reduciría los costos de instalación.

-En ambas sedes se cuenta con 110v de la energía convencional, y no se hace uso de planta eléctrica y el único sistema de respaldo que son UPS.

1.1.2 UNICAM MADRIZ

En la sede Central de Madriz(UNICAM), se cuenta con una línea telefónica con un Acceso internet con ancho de banda de 2 MB, en esta sede se cuenta con 28 computadoras marca HP con un procesado Dual Core 1.8 GHz y una memoria RAM de 2GHz, en el cual solo 13 computadoras de estas se encuentran interconectadas. El que las 2 sede ubicadas en sedes urbanas Madriz Y Estelí cuenten con acceso a Internet nos facilita para realizar la interconexión mediante una VPN entre las 2 sedes.

CAPÍTULO II

2.1- TELEFONIA IP

La Telefonía IP difiere de la Telefonía tradicional porque no usa conmutación de circuitos, sino conmutación de paquetes. Esto significa que la información se digitaliza y se transmite a través de redes de datos o redes IP en forma de paquetes de datos. Esta forma de transmisión es eficiente debido a que la red solo se utiliza si se está transportando realmente información.

La voz es enviada en paquetes de datos a través de redes IP, pero si esta se necesita comunicar con un teléfono analógico, es necesario realizar una conversión de la información (Voz) ya sea de analógica a digital o de digital a analógica según sea el caso. Para esto se utilizan Tarjetas de Interfaz que cumplen esta función, y dependerá de donde se encuentre ubicado el Teléfono Análogo o Tradicional para saber que tarjeta utilizar (FXO=Foreign Exchange Office o FXS=Foreign Exchange Station), ya que tal como lo muestra la figura 1, si el teléfono se encuentra ubicado dentro de la red administrada por el Servidor IP, se utiliza una tarjeta de Interfaz FXS, y en el caso de que el teléfono se encuentre conectado directamente a la Red de Telefonía Tradicional, se utiliza la Tarjeta de Interfaz FXO.

Instalación de un sistema VoIP corporativo basado en Asterisk Cuando se produce la transformación de analógica a digital se aplican distintos mecanismo que permite minimizar la cantidad de datos a enviar utilizando por ejemplo, mecanismos de supresión de silencio, o diferentes codificadores (códecs) que permiten comprimir los datos a enviar.

Existen tres alternativas o tipos de comunicaciones diferentes de cómo se puede aplicar Telefonía IP utilizando un servidor de Telefonía IP que administre una red LAN ya sea con Softphone (Teléfonos IP por software), Teléfonos IP Hardware o Teléfonos Análogos o Tradicionales. Estos tipos de comunicación cada uno de los dispositivos poseen una dirección IP o un numero para lograr identificarlos en la red, tanto local (LAN) como globalmente (Internet). Estas tres alternativas son:

2.1.1 COMUNICACIÓN ENTRE SOFTPHONE O TELÉFONOS IP.

Esta comunicación se lleva a cabo de manera directa, es decir, no es necesaria la utilización de tarjetas de interfaz (FXO y FXS), como se ve en la (Figura 1) ya que las información viaja solo dentro de dispositivos y redes IP. La voz se empaqueta y se codifica si así se ha establecido (pueden no usarse códecs) y se envía. Normalmente se utilizan protocolos específicos para la comunicación como SIP o IAX2, que también se abordarán más adelante.

Figura 1 Diagrama General de Telefonía IP (VoIP)

2.1.1 COMUNICACIÓN ENTRE SOFTPHONE/VOIP A TELÉFONO ANALÓGICO

En este tipo de comunicación es necesaria la utilización de un dispositivo que permita la comunicación entre la red de datos y la red de Telefonía Tradicional. En el caso de que se quiera acceder el Teléfono Tradicional A desde un Teléfono IP o un Softphone es necesaria la tarjeta de Interfaz FXO la cual permite conectarse directamente a la PSTN. En el caso de que se quiera acceder al Teléfono Tradicional B, es necesario un Operador IP quien permite realizar llamadas a través de Internet a destinos tradicionales, es decir, logra comunicar las redes IP con la PSTN a por medio de Internet (Rodríguez, 2014).

2.1.2 COMUNICACIÓN ENTRE TELÉFONOS ANÁLOGOS

Bajo esta comunicación (Figura 2) es necesario los mismos dispositivos que en el punto anterior, es decir, la Tarjeta de Interfaz FXO y el Proveedor IP para lograr la comunicación desde el servidor IP hasta el Teléfono Tradicional, este caso el A y B. Sin embargo, también es necesaria la tarjeta de interfaz FXS, la cual permite conectar los teléfonos tradicionales o análogos al servidor para que así estos puedan comunicarse con la PSTN o directamente a la red LAN.

En las figuras se logra apreciar que el servidor de telefonía IP es muy importante ya que es quien administra la red local, con teléfonos y computadores, y permite que estos se conecten tanto con Internet como con la red de Telefonía Tradicional. Este servidor cumple la función de una centralita PBX o una central Telefónica.

Este Servidor IP, es el contendrá la Centralita (PBX) por software. Y es el encargado de establecer las conexiones entre los teléfonos o terminales de una misma empresa, o de hacer que las llamadas se cursen hacia el exterior. Son muchas las funciones que puede realizar una PBX, entre las que se pueden mencionar que posee las mismas características de un PBX tradicional, como lo es la agrupación de una cantidad de N líneas de teléfono en un único número que se muestra al público y al cual se puede llamar, manejar los números del interior de una empresa por medio de anexos, música en espera, transferencia de llamadas, llamadas en espera, entre muchas otras.

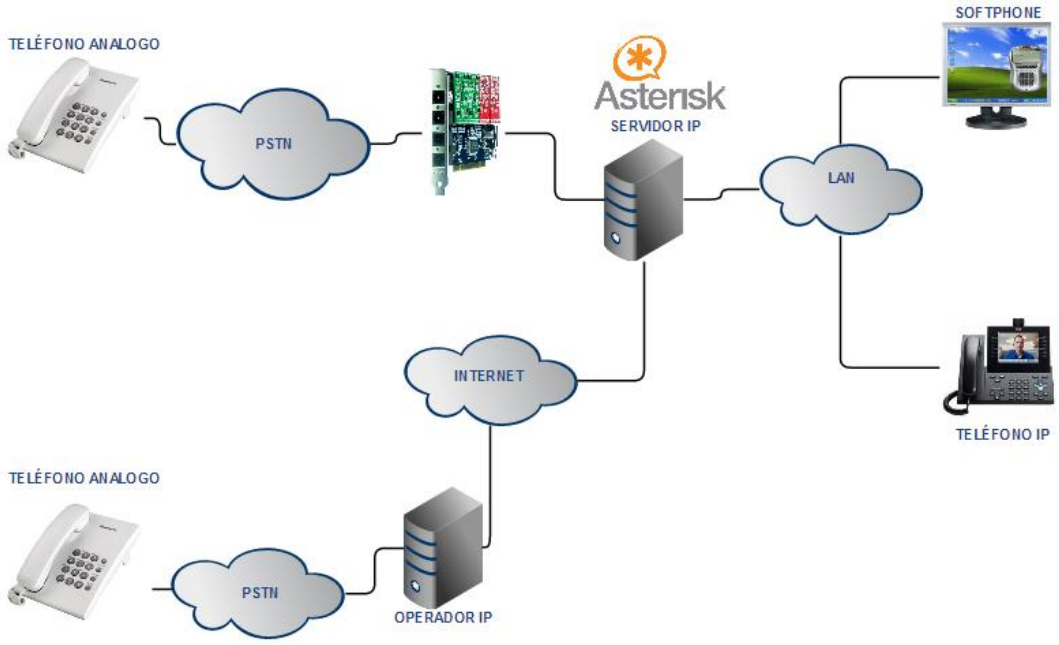


Figura 2: Red PSTN Convergente con Red VoIP

Como ya se ha mencionado existen dos interfaces que son muy importantes para combinar y poder conectar los dispositivos de VoIP con los sistemas analógicos, estos son dos:

FXO (Foreign Exchange Office): También se le denomina gateway y tal como se mencionó anteriormente es el encargado de comunicar la Red IP con la PSTN. Esta tarjeta se encuentra normalmente en el Servidor IP, aunque también existen dispositivos independientes y realiza la el cambio de la información de análoga a paquetes de datos o viceversa.

FXS (Foreign Exchange Station): Según lo descrito anteriormente esta tarjeta de Interfaz permite conectar teléfonos análogos o tradicionales a un computador, en este caso el Servidor IP. De esta manera, se pueden realizar y recibir llamadas desde teléfonos análogos tanto hacia el interior de la red LAN (ya sea a Softphone, Teléfonos IP o Teléfonos Análogos conectados a la

Tarjeta FXS) o el exterior de esta red, como puede ser la PSTN u otra Red IP. Estos interfaces son conocidos como ATA's.

Ambos interfaces se pueden encontrar de diferentes formas para poder adaptarse a las necesidades de nuestra red, así existen tarjetas con n puertos FXS o de n puertos FXO o una combinación de ambos, así como existen dispositivos independientes con un puerto Ethernet y que permiten interconectarse a nuestra infraestructura sin necesidad de un servidor PBX. (Falcón, 2007)

2.1.3 FACTORES INFLUYENTES EN TRANSMISION VOIP

La transmisión de voz sobre redes IP, sufre algunas deficiencias que existen en transmisión sobre redes IP, que en el caso de la voz por su naturaleza, (necesidad de orden en la entrega de paquetes, tasa de entregas constante, etc...) se pueden convertir en factores que impidan su correcta comunicación.

Hay que recordar que, IP es un protocolo de transporte de datagramas en el que no se asegura la llegada de paquetes, ni su orden, por lo que debido a esto, en una comunicación de voz se pueden producir problemas.

El transporte de voz sobre IP se ve afectado, entre otros, por los siguientes factores que deben ser muy tenidos en cuenta a la hora de diseñar una infraestructura de VoIP para minimizarlos lo máximo posible.

Los principales factores son:

✓ **Pérdida de paquetes**: Se producen en las redes IP, principalmente por congestión de en la redes o por fallos de comunicación. Y por perdidas, no se refiere solo a la perdida completa del paquete, que no llega a destino, sino a la llegada de paquetes después de un tiempo determinado, lo que provoca que el paquete sea inservible y es por tanto descartado.

Los diferentes codecs pueden predecir los paquetes perdidos y remplazarlos, de esta manera, no se puede percibir que falto un paquete. Pero cuando esta pérdida es superior al 5%, los codecs implementados no pueden predecir el

valor del paquete perdido y se notara en la comunicación de voz que este paquete falta, disminuyendo la calidad de la comunicación.

Cuando la pérdida de paquetes es inferior al 5 % los diferentes códec utilizados pueden corregir el error.

Los codecs pueden:

- **Intrapolar:** cuando falta un paquete, el códec, toma el paquete anterior y el paquete siguiente y calcula el valor del paquete faltante.
- **Sustituir:** cuando el códec detecta un paquete faltante lo remplaza por un paquete igual al paquete anterior.

✓ **Jitter:** El Jitter es la variación en el retardo. En términos simples, es la diferencia entre el tiempo en que llega un paquete y el tiempo en que se cree que llegara el paquete. Entrando más en el funcionamiento de TCP/IP se da por hecho que los paquetes no llegan a su destino en orden y mucho menos a una velocidad constante, pero el audio tiene que tener una velocidad constante. Para obtener una buena calidad se recomiendan valores de Jitter menores de 100 ms. Para corregir el Jitter existen los “jitter buffer”, estos buffer puede manejar unos 300 milisegundos de diferencia y controlar esta variación para que el audio se escuche a velocidad constante.

Si la llegada de paquetes es demasiado desigual el buffer no la alcanza a controlar y perderá paquetes, deteriorando la calidad de la voz.

✓ **Retardo o Latencia:** El retardo es la diferencia que existe entre el momento en que una señal es trasmitida y el momento que una señal llega a su destino.

El retardo puede ser de dos tipos:

- **Constante:** Dentro de las fuentes de retardo constante están todas aquellas que siempre generan la misma cantidad de retardo, las más importantes son:

  - **Codificación:** es el retardo generado al tomar el audio y procesarlo por un códec específico.

- **Paquetización:** es el retardo generado al tomar el audio y convertirlo en paquetes IP.
- **Serialización:** es el retardo generado al colocar los paquetes de voz, desde las capas de aplicación hasta la interface por la cual será trasmitido.

- **Variable:** Las fuentes de retardo variable son todas aquellas que generan diferentes cantidades de retardo según las condiciones del medio, las más importantes son:

- **Encolamiento:** el retardo por encolamiento es el que se genera cuando los paquetes de voz tienes que esperar en las colas de los equipos activos a ser trasmitidos.
- **Supresores de eco:** - Consiste en evitar que la señal emitida sea devuelta convirtiendo por momentos la linea full-duplex en una línea halfduplex de tal manera que si se detecta comunicación en un sentido se impide la comunicación en sentido contrario. El tiempo de conmutación de los supresores de eco es muy pequeño. Impide una comunicación fullduplex plena.

- **Canceladores de eco:** Es el sistema por el cual el dispositivo emisor guarda la información que envía en memoria y es capaz de detectar en la señal de vuelta la misma información (tal vez atenuada y con ruido). El dispositivo filtra esa información y cancela esas componentes de la voz (Rodríguez, 2014).

2.1.4 PROTOCOLOS DE SEÑALIZACIÓN

Un protocolo es un conjunto de reglas y acuerdos que los computadores y dispositivos deben seguir para que puedan comunicarse entre ellos. Más concretamente, un protocolo de señalización es el que se encarga de gestionar los mensajes y procedimientos utilizados para establecer una comunicación.

Para VoIP existen varios protocolos de señalización, tales como, H323, MGCP, SCCP, SIP y IAX2. Sin embargo, los tres protocolos más extendidos

son SIP, IAX2, y H323. Aunque H323 ha estado muy extendido, ha sido muy utilizado y ha sido el que ha permitido el despegue de la VoIP, existiendo gran variedad de hardware que lo soporta, hoy en día, está en desuso, ya que uno de los objetivos de SIP era solucionar los problemas que existían en H323, por lo que SIP ha desbancado a H323.

Básicamente H323 es un protocolo cliente-servidor en el que básicamente intervienen dos tipos de señalización: Señalización de control de llamada (H225) y Señalización de control de canal (H245), la primera se encarga del registro y localización y la segunda del establecimiento de llamadas.

A continuación se verá detalladamente los dos más importantes, que son además, los que vamos a utilizar en nuestra propuesta: SIP y IAX2. (VoipForo, 2014)

2.1.5 SIP (Session Initiation Protocol)

Este protocolo está más integrado con las aplicaciones y servicios de Internet, posee mayor flexibilidad para incorporar nuevas funciones y su implementación es mucho más simple que H323, incluso es parecido a los protocolos HTTP y SMTP.

Las aplicaciones SIP usan el puerto 5060 con UDP (User Datagram Protocol) o TCP (Transmission Control Protocol), para información de señalización y normalmente el rango de puertos de 10000 a 20000, para la transmisión de la voz mediante RTP, más concretamente se usan dos puertos por canal de comunicación.

SIP se ha propuesto como sistema genérico para el soporte de mecanismo de señalizaciones de servicio de telefonía IP. SIP soporta cinco elementos funcionales para el establecimiento y terminación de comunicaciones multimedia:

- ➢ Localización de Usuarios.
- ➢ Intercambio y negociación de capacidades de los terminales.
- ➢ Disponibilidad de Usuarios.

➢ Establecimiento de llamadas.

➢ Mantenimiento de llamadas.

SIP es un protocolo basado en el modelo cliente-servidor. Los clientes SIP envían peticiones aun servidor, el cual una vez procesada contesta con una respuesta. Los terminales SIP, también pueden establecer llamadas de voz directamente sin la intervención de elementos intermedios, al igual que en el caso de H323, funcionando como “peers independientes”.

SIP se estructura con los siguientes componentes:

1. AGENTES DE LLAMADA: Existen dos tipos de Agentes:

➢ User Agent Client (UAC): funciona como cliente iniciando peticiones SIP.

➢ User Agent Server (UAS): funciona como servidor contactando al usuario cuando una petición SIP es recibida, y retornando una respuesta a favor del usuario.

Estos agentes realizan las siguientes acciones:

➢ Localizar a un usuario mediante la redirección de la llamada.

➢ Implementar servicios de redirección como reenvío si no hay respuesta.

➢ Implementar filtrado de llamadas en función de su origen o destino.

➢ Almacenar información de administración de llamadas.

Las workstations, IPphones, gateways telefónicos, call agents, entre otros, son dispositivos que tienen funcionalidades de User Agents dentro de una red SIP.

SERVIDORES: Existen tres tipos de servidores, que pueden estar separados o realizar varias funciones.

I. Servidor Proxy: Se encarga de encaminar peticiones/respuestas hacia el destino final. El encaminamiento se realiza salto a salto de un servidor a otro hasta alcanzar el destino final. Un servidor proxy es una entidad intermediaria en una red SIP que es responsable de reenviar peticiones SIP a un UAS (User Agent Server) de destino o a otro servidor proxy en nombre de otro UAC (User Agent Client). El servidor proxy también interpreta y si es necesario, reescribe partes de los mensajes de petición antes de reenviarlos. También se asegura de poner en funcionamiento las políticas en la red, tales como autenticar a un usuario antes de darle servicio.

II. Servidor de redirección: Equivalente al servidor proxy, pero a diferencia de este no contesta a la llamada, sino que indica como contactar el destino buscado. Un redirect server, es un UAS (User Agent Server) que se encarga de redireccionar las transacciones SIP generadas por un UAC. Para esto genera respuestas a peticiones SIP con código 300 (mensajes de redirección), dirigiendo al UAS a contactar a un grupo alternativo.

III. Servidor de registro: Mantiene la localización actual de un usuario. Se utiliza para que los terminales registren la localización en la que se encuentran, facilitando la movilidad del usuario.

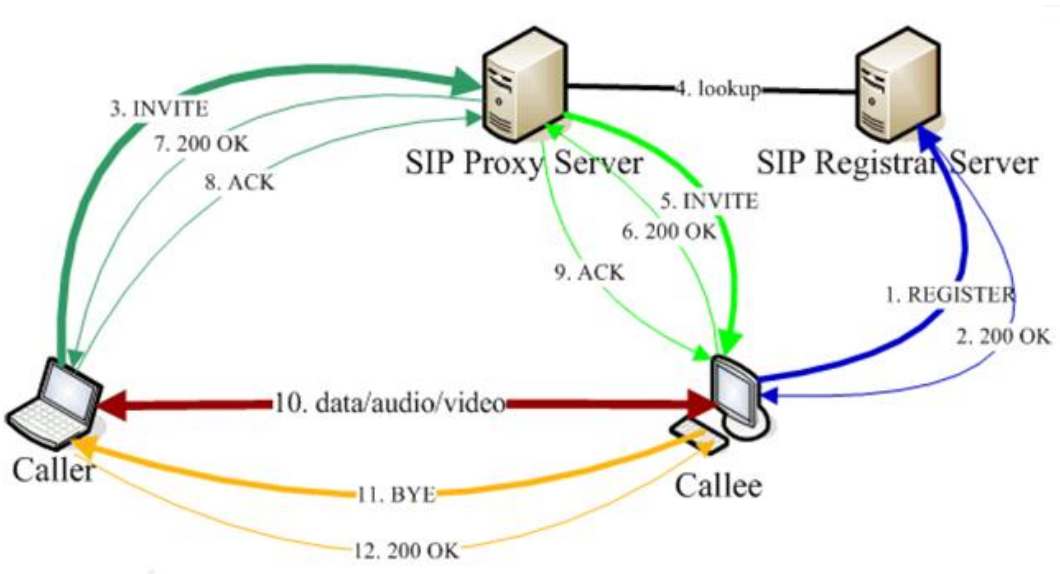


Figura 3: Proceso De Una Comunicación Vía SIP

Como ya hemos comentado, SIP está basado en arquitectura cliente/servidor similar al HTTP, con el que comparte muchos códigos de estado y sigue una estructura de Figura 3: Llamada mediante SIP Instalación de un sistema VoIP corporativo basado en Asterisk petición-respuesta; estas peticiones son generadas por un cliente y enviadas a un servidor, que las procesa y devuelve la respuesta al cliente. El par petición-respuesta recibe el nombre de transacción. Al igual que el protocolo HTTP, SIP proporciona un conjunto de solicitudes y respuestas basadas en códigos, todas ellas recogidas en la RFC 3261.

2.1.7- IAX

Este protocolo es utilizado para manejar conexiones VoIP ya sea entre servidores Asterisk, o entre servidores y clientes. El protocolo IAX ahora se refiere generalmente al IAX2, la segunda versión del protocolo IAX2.

IAX2 fue creado y estandarizado en Enero de 2004 por Mark Spencer y su empresa Digium, la creadora de Asterisk, y es creado para y por Asterisk. Y surge también, para corregir algunos de los problemas principales del protocolo SIP, estos objetivos son:

✓ Minimizar el ancho de banda usado en las transmisiones de control y multimedia.

✓ Cambiar de protocolo de texto a protocolo binario. Pequeñas cabeceras y bajo consumo de ancho de banda.

✓ Evitar problemas de NAT (Network Address Translation). IAX2 usa UDP sobre un único puerto, el 4569, donde viajan la información de señalización y datos.

✓ Soporte para transmitir planes de marcación (dialplans).

IAX2 soporta la autentificación de estilo PKI (Public Key Infraestructure) y trunking.

IAX2 realiza autenticación en llamadas entrantes y salientes. En cuanto a seguridad, éste permite la autentificación, y en ciertas situaciones cifrado

entre terminales.Al hacer trunking con IAX2 solamente el ancho de banda usado se asigna siempre.

Otros protocolos usados para el trunking asignan siempre cierta cantidad de ancho de banda para mantener todos los canales abiertos. El trunking de IAX2 permite que los streams múltiples de voz compartan un solo “trunk” a otro servidor, reduciendo así las sobrecargas creadas por los paquetes de IP. El trunking requiere que ambos lados se conozcan, es decir, si un lado tiene trunk=yes y el otro no, se conseguirá solo audio unidireccional.

IAX2 utiliza un único puerto UDP, generalmente el 4569, para comunicaciones entre puntos finales (terminales VoIP) para señalización y datos. El tráfico de voz es transmitido in-band (junto con la voz), lo que hace a IAX2 un protocolo casi transparente a los cortafuegos y realmente eficaz para trabajar dentro de redes internas. En esto se diferencia de SIP, que utiliza una cadena RTP out-of-band para entregar la información.

IAX2 soporta Trunking, donde un simple enlace permite enviar datos y señalización por múltiples canales. Cuando se realiza Trunking, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia adicional; esto es una gran ventaja para los usuarios de VoIP, donde las cabeceras IP son un gran porcentaje del ancho de banda utilizado, además de que permite reducir la latencia y el jitter.

En IAX2 existen dos tipos de tramas, esto es así, para optimizar el ancho de banda utilizado, sobre todo cuando está establecida la comunicación, y se está transmitiendo voz, momento en el que las cabeceras de los paquetes no necesitan mucha información y deben ser mínimas. Existen dos tipos de tramas:

➢ **Tramas F o Full Frames:** La particularidad de las tramas o mensajes F es que deben ser respondidas explícitamente. Contienen una cabecera con numerosos campos.

➢ **Tramas M o Mini Frames**: Las tramas M o mini frames sirven para mandar la información con la menor información posible en la cabecera.

Estas tramas no tienen por qué ser respondidas y si alguna de ellas se pierde se descarta sin más.

c) SIP Vs. IAX - Comparativa

Las principales diferencias ente IAX y SIP son las siguientes:

- **Ancho de banda:** IAX utiliza un menor ancho de banda que SIP ya que los mensajes son codificados de forma binaria mientras que en SIP son mensajes de texto. Asimismo, IAX intenta reducir al máximo la información de las cabeceras de los mensajes reduciendo también el ancho de banda necesario.
- **NAT:** En IAX la señalización y los datos viajan conjuntamente con lo cual se evitan los problemas de NAT que frecuentemente aparecen en SIP. En SIP la señalización y los datos viajan de manera separada y por eso aparecen problemas de NAT en el flujo de Instalación de un sistema VoIP corporativo basado en Asterisk audio cuando este flujo debe superar los routers y firewalls. SIP suele necesitar un servidor STUN para estos problemas.
- **Estandarización y Uso:** SIP es un protocolo estandarizado por la IETF hace bastante tiempo y que es ampliamente implementado por todos los fabricantes de equipos y software. IAX está aún siendo estandarizado y es por ello que no se encuentra en muchos dispositivos existentes en el mercado.
- **Utilización de puertos:** IAX utiliza un solo puerto (4569) para mandar la información de señalización y los datos de todas sus llamadas. Para ello utiliza un mecanismo de multiplexación o "trunking". SIP, sin embargo utiliza un puerto (5060) para señalización y 2 puertos RTP por cada conexión de audio (como mínimo 3 puertos). Por ejemplo para 100 llamadas simultáneas con SIP se usarían 200 puertos (RTP) más el puerto 5060 de señalización. IAX utilizaría sólo un puerto para todo (4569).
- **Flujo de audio al utilizar un servidor :** En SIP si se utiliza un servidor la señalización de control pasa siempre por el servidor pero la

información de audio (flujo RTP) puede viajar extremo a extremo sin tener que pasar necesariamente por el servidor SIP. En IAX al viajar la señalización y los datos de forma conjunta todo el tráfico de audio debe pasar obligatoriamente por el servidor IAX. Esto produce un aumento en el uso del ancho de banda que deben soportar los servidores IAX sobre todo cuando hay muchas llamadas simultáneas.

- **Otras funcionalidades:** IAX es un protocolo pensado para VoIP y transmisión de vídeo y presenta funcionalidades interesantes como la posibilidad de enviar o recibir planes de marcado (dialplans) que resultan muy útiles usados junto con servidores Asterisk. SIP es un protocolo de propósito general y podría transmitir sin dificultad cualquier información y no solo audio y vídeo, pero no funciona de manera tan óptima como lo hace IAX2 (Rodríguez, 2014).

2.1.8 SOFTWARE DE SERVIDOR DE VOIP

Existe varias soluciones software de código abierto que implementan las funciones de una centralita (PBX), las más populares son: OpenPBX, PBX4Linux, YATE, FreeSwitch y Asterisk.

De entre ellas, la más extendida, popular, que ofrece mayor número de dispositivos hardware y que proporciona mayor número de aplicaciones de terceros para ampliar sus funcionalidades es Asterisk. Así que debido a su superioridad respecto a las otras soluciones solo se tratará con el mismo.

Asterisk es una PBX (Phone Box eXchanger) software. Es decir, una Centralita Telefónica por Software. Es software libre (Open Source), desarrollado principalmente por la empresa DIGIUM. Su código se encuentra publicado bajo licencia GPL, y fue creado en c bajo Linux.

Se ejecuta en un PC standar (arquitectura x86, amd64, ppc) bajo GNU/Linux, BSD, Sun Solaris, o MacOSX. Soporta todas las funcionalidades de las centralitas hardware, incluso algunas características avanzadas de grandes centralitas propietarias programables, y además de ofrecer interfaces para poder crear nuevas funcionalidades adaptadas al usuario.

Actualmente, la empresa Digium, fundada por Mark Spencer y sucesora de Linux- Support, administra y mantiene el código fuente de Asterisk, y lo ofrece bajo dos licencias: GPL y licencia comercial. Digium vende Hardware creado especialmente para Asterisk, tarjetas analógicas y digitales las cuales son soportadas por los drivers ZAP, incluidos por defecto en Asterisk.

Asterisk es una solución probada y robusta, tanto para pequeñas instalaciones como para proveedores o carriers. Algunas de las funciones básicas que asterisk ofrece son: Transferencia Música en espera, Registro de llamadas en MySql, Transferencia Atendida, Música en transferencia, Buzón de Voz por Mail, Llamada en espera, Salas de Conferencia, Captura de llamadas, Desvío si ocupado, Bloqueo de Caller ID, Colas de llamada, Desvío si no responde, Timbres distintivos, Colas con prioridad.

Otras funciones más avanzas que ofrece son:

✓ IVR: Interactive Voice Response, gestión de llamadas con menús interactivos.

✓ LCR: Least Cost Routing, encaminamiento de llamadas por el proveedor VoIP más económico.

✓ AGI: Asterisk Gateway Interface, integración con todo tipo de aplicaciones externas.

✓ AMI: Asterisk Management Interface, gestión y control remoto de Asterisk.

✓ BB.DD: Base de datos, usuarios, llamadas, extensiones, proveedores...

Asterisk además de soportar diferentes tarjetas analógicas y digitales, también admite diferentes protocolos de señalización, lo que le permite una gran flexibilidad.

A continuación se muestran diferentes puntos del funcionamiento de Asterisk para comprender mejor que no ofrece, como se estructura y como funciona:

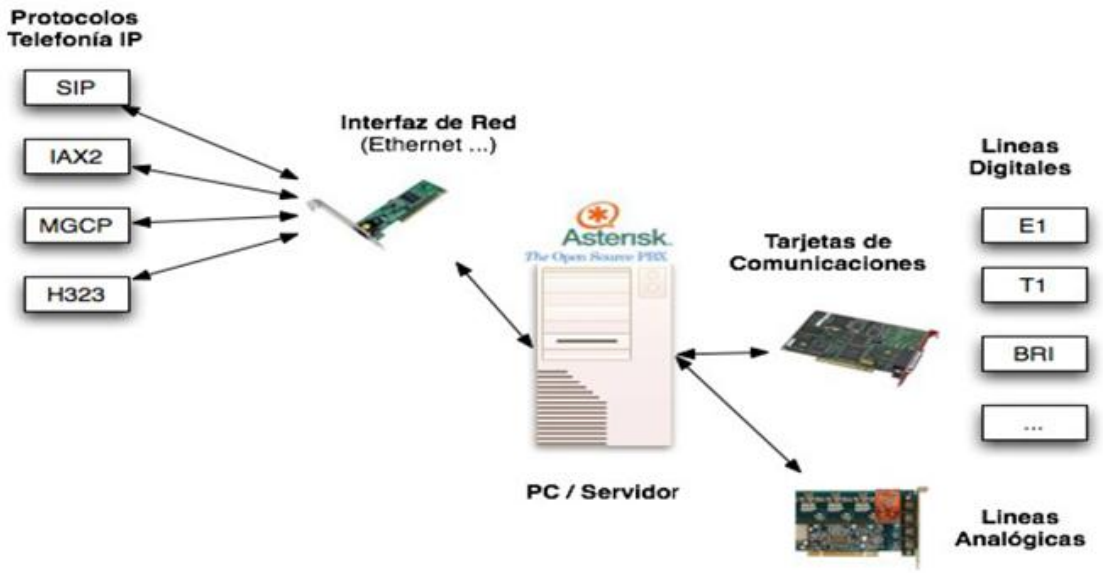


Figura 4: Servidor Asterisk, Protocolos y Hardware

a) Estructura de Directorios y Funcionamiento

Asterisk es un “demonio” que se ejecuta en segundo plano en sistemas Linux. La configuración se almacena en varios ficheros de texto editables de forma tradicional. Se distribuye como código fuente para ser compilado e instalado, y además existen versiones 'paquetizadas' para las distribuciones GNU/Linux más comunes. La estructura de directorios en la que se instala Asterisk es la siguiente:

➢ Binarios asterisk: /usr/sbin/asterisk

➢ Módulos ejecutables de asterisk: /usr/lib/asterisk/modules

➢ Voces pregrabadas: /var/lib/asterisk/sounds

➢ Ficheros de Configuración: /etc/asterisk/ *.conf

➢ Otros Servicios (Buzón de Voz,....): /var/spool/asterisk/

➢ Proceso activo: /var/run

Esta es la estructura en cuanto a la instalación física en un sistema Linux, en el siguiente apartado se verá su estructura lógica, y como esta es modular.

b) Estructura

Asterisk se integra varios componentes, de estos los que se instalan por defecto son los siguientes:

– Asterisk: Núcleo (core) del sistema.

– Asterisk-sounds: Voces de calidad pregrabadas y formatos de audio.

– Asterisk-addons: Software adicional (CSV,FreeTDS, etc ...)

– Libpri: Librería para gestionar enlaces RDSI Primarios.

– Libiax: Librería para utilizar el protocolo IAX.

– Zaptel: Interfaz del Kernel para acceder a tarjetas analógicas o digitales.

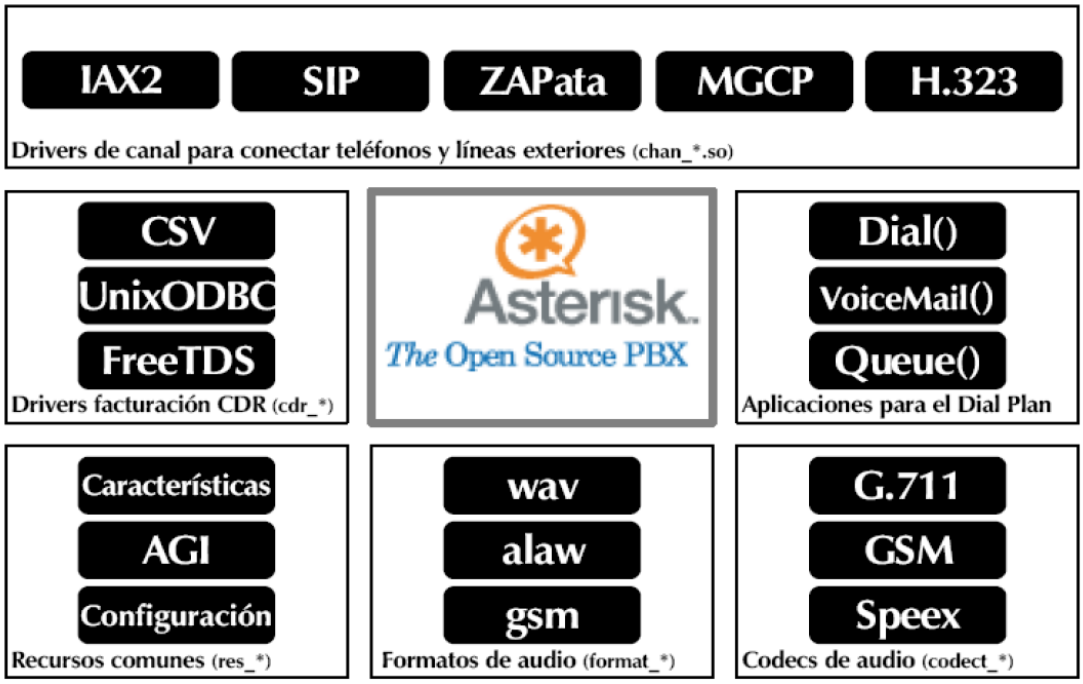


Figura 5: Códecs, Aplicaciones y Formatos Soportados por Asterisk

Y éstos componentes a su vez en, en diferentes módulos, como se puede observar en la Figura 5.

✓ **API de canales:** Sirve para controlar todas las llamadas del sistema, sean Voz IP, analógicas cualquier otra tecnología pudiendo desarrollar nuevos canales

✓ **API de Formato de Ficheros:** Sirve para controlar el formato de ficheros que pueden ser controlados por el sistema

✓ **API de Aplicaciones:** Se han desarrollado muchas aplicaciones de IVR, MultiConferencia, etc. Pudiendo desarrollar todas aquellas aplicaciones más mediante AGI (Asterisk Gateway Interface) en C, C++, perl, php, etc.

✓ **API de Traducción de Codec:** Controla la traducción de códec entre participantes en una comunicación. Se pueden implementar códec nuevos. (3CX, 2014)

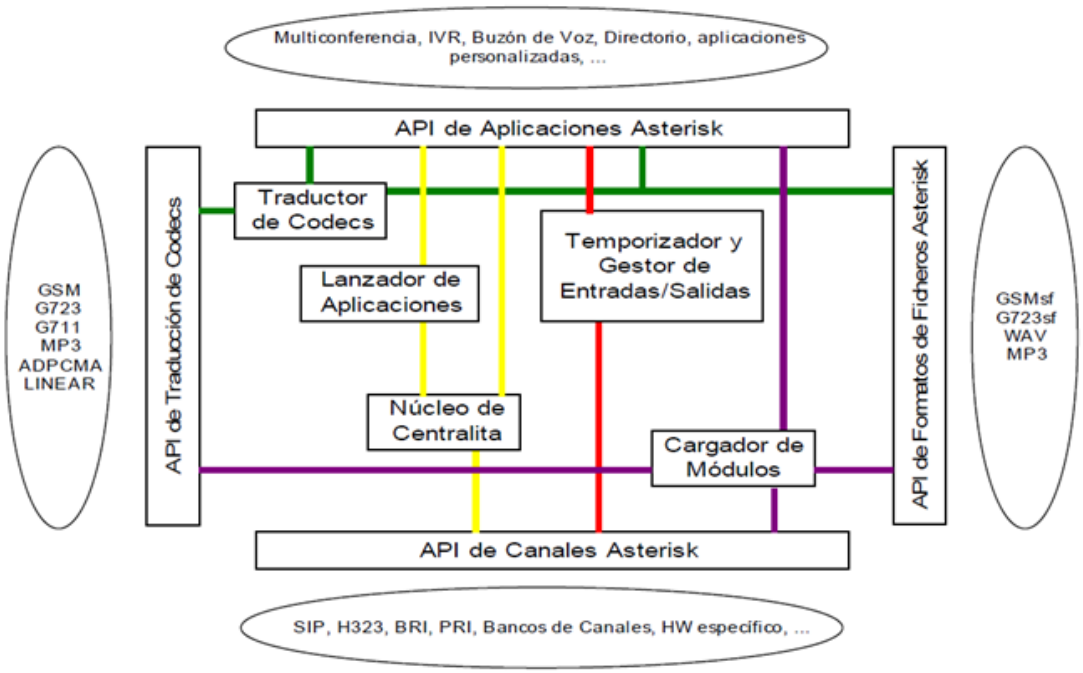


Figura 6: Estructura de Asterisk

Conceptos de Asterisk

➢ **Canal:** Es una conexión que conduce una llamada entrante o saliente en el sistema Asterisk. La conexión puede venir o salir hacia telefonía tradicional analógica o digital o VozIP. Por defecto, Asterisk soporta una serie de canales, los más importantes:

– Protocolos VozIP: H.323, IAX2, SIP, MGCP

– Console: GNU Linux OSS/ALSA sound system.

– Zap: Lineas analógicas y digitales.

➢ **Dialplan:** Se trata de la configuración de la centralita Asterisk que indica el itinerario que sigue una llamada desde que entra o sale del sistema hasta que llega a su punto final. Se trata en lineas generales del comportamiento lógico de la centralita.

➢ **Extensión:** En telefonía tradicional, las extensiones se asocian con teléfonos, interfaces o menús. En Asterisk, una extensión es una lista de comandos a ejecutar.

➢ **Contexto (Context):** El Dialplan o lógica de comportamiento de Asterisk se divide en uno o varios contextos. Un contexto es una colección de extensiones.

➢ **Aplicación (Application):** Asterisk ejecuta secuencialmente los comandos asociados a cada extensión. Esos comandos son realmente aplicaciones que controlan el comportamiento de la llamada y del sistema en sí (Rodríguez, 2014). (Asterisk, 2014)

2.2- VPN

VPN (Virtual Private Network) es una extensión de una red local y privada que utiliza como medio de enlace una red pública como por ejemplo, Internet. También es posible utilizar otras infraestructuras WAN tales como Frame Relay, ATM, etc. Este método permite enlazar dos o más redes simulando una única red privada permitiendo así la comunicación entre computadoras como si fuera punto a punto. También un usuario remoto se puede conectar individualmente a una LAN utilizando una conexión VPN, y de esta manera utilizar aplicaciones, enviar datos, etc. de manera segura.

Las Redes Privadas Virtuales utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, esto es importante a la hora de diferenciar Redes Privadas Virtuales y Redes Privadas, ya que esta última utiliza líneas telefónicas dedicadas para formar la red. Una de las principales ventajas de una VPN es la seguridad, los paquetes viajan a través de infraestructuras públicas (Internet) en forma encriptada y a través del túnel de manera que sea prácticamente ilegible para quien intercepte estos paquetes.

Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas, por ejemplo diferentes ciudades y a veces hasta piases y continentes.

Por ejemplo empresas que tienen oficinas remotas en puntos distantes, la idea de implementar una VPN haría reducir notablemente los costos de comunicación, dado que las llamadas telefónicas (en caso de usar dial-up) serían locales (al proveedor de Internet) o bien utilizar conexiones DSL, en tanto que de otra manera habría que utilizar líneas dedicadas las cuales son muy costosas o hacer tendidos de cables que serían más costosos aun.

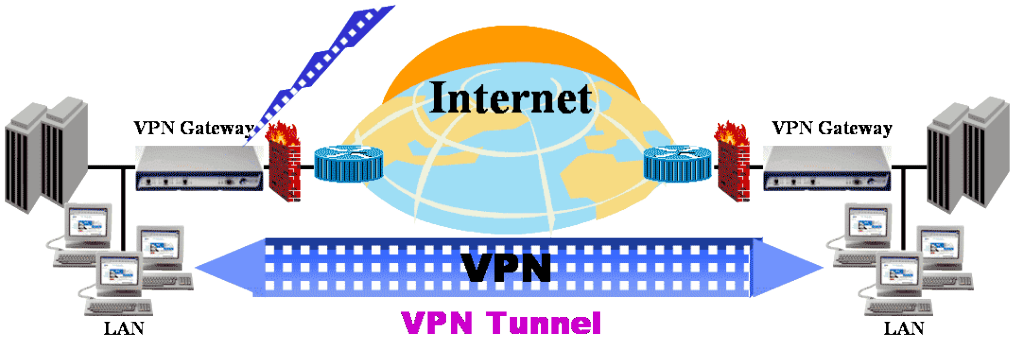


Figura 7: Esquema Lógico de una VPN (Caire, 2014)

2.2.1- VENTAJAS DE UNA VPN

Seguridad: Una de red de este tipo provee encriptación y encapsulación de datos de manera que hace que estos viajen codificados y a través de un túnel. Es importante señalar que los datos que viajan a través de la VPN se trasladan encriptados, por lo que sólo podrán acceder a ellos los usuarios de dicha VPN, garantizando así la privacidad de los datos.

Costos: Las VPN ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.

Mejor administración: Cada usuario que se conecta puede tener un numero de IP fijo asignado por el administrador, lo que facilita algunas tareas como por ejemplo mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.

Facilidad: Los usuarios con poca experiencia podrán conectarse a grandes redes corporativas transfiriendo sus datos de forma sencilla y segura. (Caire, 2014), (Informatica Hoy, 2014)

2.2.2- TIPOS DE VPN

Las formas en que pueden implementar las VPNs pueden ser basadas en HARDWARE o a través de SOFTWARE, pero lo más importante es el protocolo que se utilice para la implementación. Las VPNs basadas en HARDWARE utilizan básicamente equipos dedicados como por ejemplo los routers, son seguros y fáciles de usar, ofreciendo gran rendimiento, a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios, en síntesis, los equipos dedicados son de fácil implementación y buen rendimiento, solo que las desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son PROPIETARIOS. Entre los más utilizados están IPSEC (Internet Protocol Security Tunnel Mode) y PPTP (Point to Point Tunneling Protocol), aunque a este último se le conocen fallas de seguridad. (Caire, 2014)

1.2.3- OPENVPN

OpenVPN es una solución para VPN que implementa conexiones de capa 2 o 3, su modelo de seguridad se basa en SSL/TLS (Secure Socket Layer/ Transport Layer Security) para cifrar y ESP (Encapsulating Security Payload) para autenticación. A pesar de que hay muy pocos fabricantes de hardware que lo integren en sus soluciones, en sistemas basados en Linux, incluso en Windows se puede implementar sin problemas mediante software. Ofrece una combinación de seguridad a nivel empresarial, seguridad, facilidad de uso y riqueza de características. Es una solución multiplataforma que ha simplificado la configuración de VPN's frente a otras soluciones más antiguas y difíciles de configurar como IPSEC y haciéndola más accesible para el público en este tipo de tecnología.

Cada integrante tiene dos llaves, una pública y otra privada. La pública es distribuida y usada por cualquiera para cifrar los datos que serán enviados a la contraparte quien conoce la llave privada que es imprescindible para descifrar los datos. El par de llave pública/privada es generado a partir de algoritmos matemáticos que aseguran que solo con la llave privada es posible leer los datos originales. Las bibliotecas SSL/TLS son parte del software OpenSSL que viene instalado en cualquier sistema moderno e

implementa mecanismos de cifrado y autenticación basados en certificados. Los certificados generalmente son emitidos por entidades de reconocida confiabilidad aunque también pueden ser emitirlos por nosotros mismos y se pueden utilizar en nuestra propia VPN. Con un certificado firmado, el dueño del mismo es capaz de demostrar su identidad a todos aquellos que confíen en la autoridad certificadora que lo emitió. (Wikipedia, 2014)

2.2.4- OPENVPN VS IPSEC

IPsec	OpenVPN
Estándar de la tecnología VPN	No compatible con IPsec
Plataformas de hardware (dispositivos, aparatos)	Solo en computadoras, pero en todos los sistemas operativos disponibles, también hay dispositivos que integran OpenVPN
Tecnología conocida y probada	Probada y sigue en crecimiento
Muchas interfaces gráficas disponibles	Sin interfaces gráficas profesionales, aunque ya existen algunos proyectos prometedores
Modificación compleja del stack IP	Tecnología sencilla
Necesidad de modificaciones críticas al kernel	Interfaces de red y paquetes estandarizados
Necesidad de permisos de administrador	Ejecuta en el espacio del usuario y puede ser chroot-ed
Diferentes implementaciones pueden ser incompatibles entre si	Tecnologías de cifrado estandarizadas
Configuración compleja y tecnología compleja	Facilidad, buena estructuración, tecnología modular y facilidad de configuración
Curva de aprendizaje muy pronunciada	Fácil de aprender e implementar
Necesidad de uso de múltiples puertos y protocolos en el firewall	Utiliza sólo un puerto del firewall
Problemas con direcciones dinámicas en ambas puntas	Trabaja con servidores de nombres dinámicos como DynDNS o No-IP con reconexiones rápidas y transparentes
Problemas de seguridad de las tecnologías IPsec	SSL/TLS como estándar de criptografía
	Control de tráfico (Traffic shaping)
	Más de 20 Mbps en máquinas de 1Ghz
	Compatibilidad con firewall y proxies
	Ningún problema con NAT (ambos lados puede ser redes NATeadas)

2.2.5- REQUERIMIENTOS PARA EL ARMADO DE UNA VPN

Para el correcto armado de una VPN, es necesario cumplir con una serie de elementos que a continuación se detallan:

- Tener una conexión a Internet: ya sea por conexión IP dedicada, ADSL o dial-up.
- Servidor VPN: básicamente es una pc conectada a Internet o un dispositivo dedicado esperando por conexiones de usuarios VPN y si estos cumplen con el proceso de autenticación, el servidor aceptara la conexión y dará acceso a los recursos de la red interna.
- Cliente VPN: este puede ser un usuario remoto o un enrutador de otra.
- Asegurarse que la VPN sea capaz de:
    - ✓ Encapsular los datos
    - ✓ Autentificar usuarios.
    - ✓ Encriptar los datos.
    - ✓ Asignar direcciones IP de manera estática y/o dinámica. (Caire, 2014)

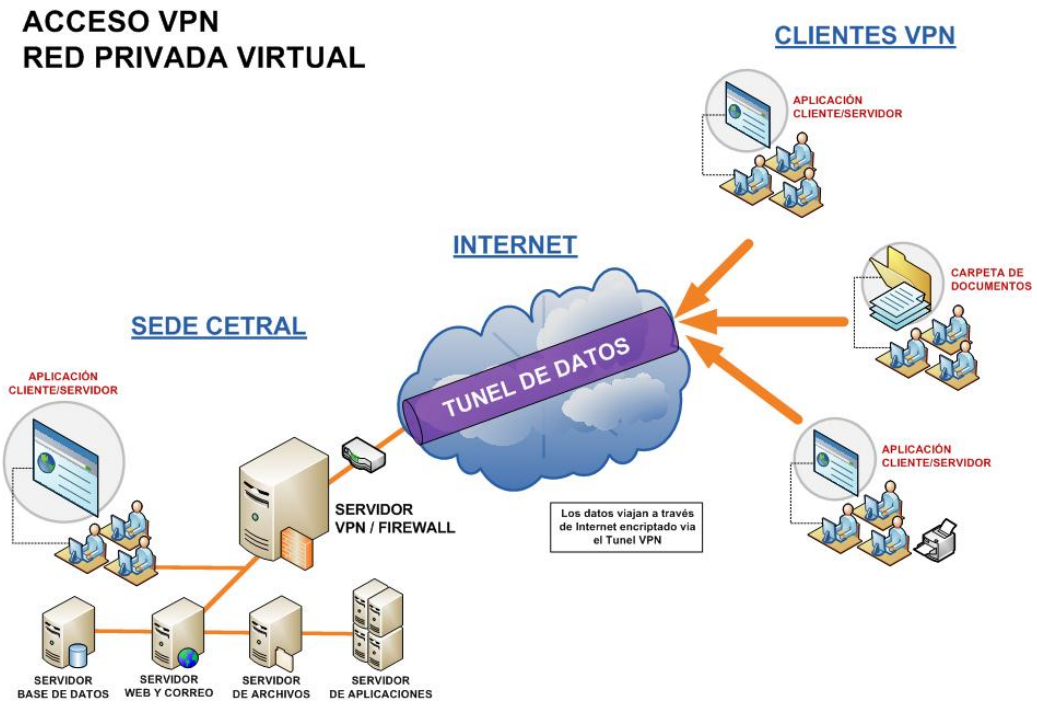


Figura 8: Acceso VPN (Soluciones de Tecnología Linux,2014)

2.3- RADIOENLACE

2.3.1- LAS MICROONDAS

La ingeniería moderna de las Microondas es un campo bastante amplio y dinámico, debido en gran parte a la convergencia entre los recientes avances de la tecnología en los dispositivos electrónicos modernos y al estallido de la demanda de los servicios de voz, datos, y la capacidad de comunicación mediante vídeo que se inició en la década de 1990 y que continúa hasta el presente. Antes de esta revolución en las comunicaciones, la tecnología de microondas fue de dominio casi exclusivo de la industria de la defensa; El reciente y dramático aumento de la demanda de sistemas de comunicación para aplicaciones tales como la paginación inalámbrica, telefonía móvil, transmisión de video, y las redes de ordenadores ha revolucionado la industria de las Microondas.

Estos sistemas de comunicación se emplean en una amplia gama de entornos, incluyendo las oficinas corporativas, instalaciones industriales y de manufactura, infraestructura para los municipios, así como viviendas particulares. La diversidad de aplicaciones y entornos operativos ha llevado a la producción en masa de esta tecnología, con un enfoque de eficiencia que a su vez está directamente proporcional al costo.

Dentro de las diferentes aplicaciones de las microondas están los sistemas de radar para evitar colisiones auto-motrices, el acceso a servicios digitales de banda ancha a través de estas, entre otras. La tecnología de microondas se adapta de forma natural para estas aplicaciones emergentes de comunicaciones y detección, ya que las altas frecuencias operativas permiten un gran número de canales independientes para una amplia variedad de usos, así como el ancho de banda disponible por canal, para una comunicación a altas velocidades.

El término "ingeniería de microondas", se utiliza para referirse al diseño e implementación de sistemas electrónicos con frecuencias de operación en el rango de los 300 MHz a los 300 GHz dentro del espectro electromagnético, con longitudes de onda que se extienden desde 1 m a 1 mm respectivamente.

En un sistema de microondas los tamaños de los componentes electrónicos típicos son a menudo comparable a la longitud de onda de la señal (λ), que además de estar directamente relacionada con la frecuencia de las señales electrónicas que serán procesadas, surge una distinción fundamentalmente de la velocidad finita de propagación de las ondas electromagnéticas (y por lo tanto, de las corrientes y voltajes).

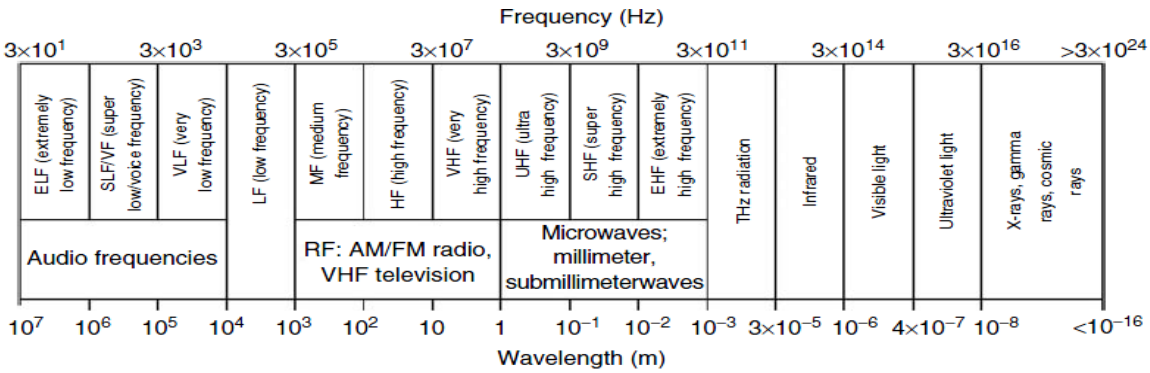


Figura 9: Espectro de Frecuencias Electromagnéticas y Longitudes de Onda Asociadas

Se decide trabajar con un enlace de microondas para interconectar el tramo de red que una dos sucursales de la institución INSFOP (en la zona rural y la zona urbana en la ciudad de Estelí) debido al difícil comunicación que tienen entre sí y a la falta de acceso las redes de comunicación, y que por esta razón se ven en la necesidad movilizarse entre las sedes para realizar las diferentes actividades o emitir orientaciones; Este enlace les permitirá estar conectados en la misma VPN (Red Privada Virtual), por lo tanto: compartir su información, internet, poder realizar llamadas internas a las diferentes extensiones y/o salir por sus troncales telefónicas para las llamadas externas, reduciendo sus costos y facilitando sus funciones. La topología que se utilizará se conoce como enlace punto a punto, cuando se refiere a una topología, se hace para representar la forma de conexionado y el flujo físico de los datos, y cuando se habla de un enlace punto a punto, se refiere a uno en el cual toda la comunicación se produce entre dos puntos (un punto Local y un punto Remoto), y sólo entre éstos; En el caso de las microondas se usarán las ondas electromagnéticas producidas por equipos electrónicos que permiten la unión de un tramo de red mediante una conexión inalámbrica, por medio de la cual se puede transportar voz, datos y multimedia. (Golio, 2008)

Figura 10: Enlace Punto a Punto

El realizar la conexión entre dos puntos por medio de microondas es todo un campo de la ingeniería en Telecomunicaciones, ya que se encontraron múltiples variables, las que se deben tener siempre en cuenta a la hora del diseño de un radio enlace; Se debe empezar considerando los servicios que serán proporcionados y la calidad que éstos ameritan , en nuestro caso se plantea transmitir video, voz y datos en ambas direcciones de la comunicación , luego tomar como referencia los presupuestos o capacidad de adquisición con la que cuenta la institución, en este caso INSFOP es una institución sin fines de lucro por lo que se deben buscar las soluciones más favorables; otros aspectos a tener en cuenta son por ejemplo: la orografía del terreno, condiciones geo climáticas, interferencia de otros sistemas, entre otras.

El Diseño se llevara a cabo utilizando el Software Profesional **PATHLOSS 5**, y el software Libre **Radio Mobile** por medio de los cuales se tendrá una visión aproximada a la realidad de nuestro enlace, pero en primera instancia es necesario conocer algunos conceptos y estándares de calidad, los cuales se ilustran utilizando gráficas y reportes generados por el Software para una mejor relación.

2.3.2- PERFIL DE TERRENO

En la planificación de un enlace de microondas en necesario disponer del perfil del terreno para determinar emplazamientos y altura de antenas, se debe tener cuidado para asegurar visión directa entre los emplazamientos y evitar reflexiones, ya que las reflexiones cancelan parte de la señal transmitida, produciendo como efecto adverso, la reducción del rango y calidad de la señal principal. Para conseguir el perfil de terreno, lo primero que se hizo obtener las coordenadas geográficas, para esto se apoyó de un sistema de GPS; En la sucursal de INSFOP en la parte rural de la ciudad de Estelí, se obtuvieron las coordenadas: 13º 4´ 32.4" N, 86º 23´ 47.3" W, y en la sucursal INSFOP ubicada en la parte urbana de la ciudad de Estelí: 13º 4´29.3" N, 86º 21´19.8" W.

Es necesario asegurar que el sistema estará instalado a una altura suficiente para prevenir que no haya obstrucciones entre la antena transmisora y receptora ,con las coordenadas obtenidas y con la ayuda de los Software , que proporcionan un mapa de elevación del vano, teniendo en cuenta la curvatura de la tierra, se modificó la altura de la antenas a unos 10 metros sobre el nivel del suelo aproximadamente, hasta obtener línea de vista entre ambos puntos, lo que es muy importante para que exista mejor propagación de las señales RF, en la siguiente imagen se muestra la ubicación de nuestro perfil de terreno. (Ingvar Henne & Per Thorvaldsen, 2002)

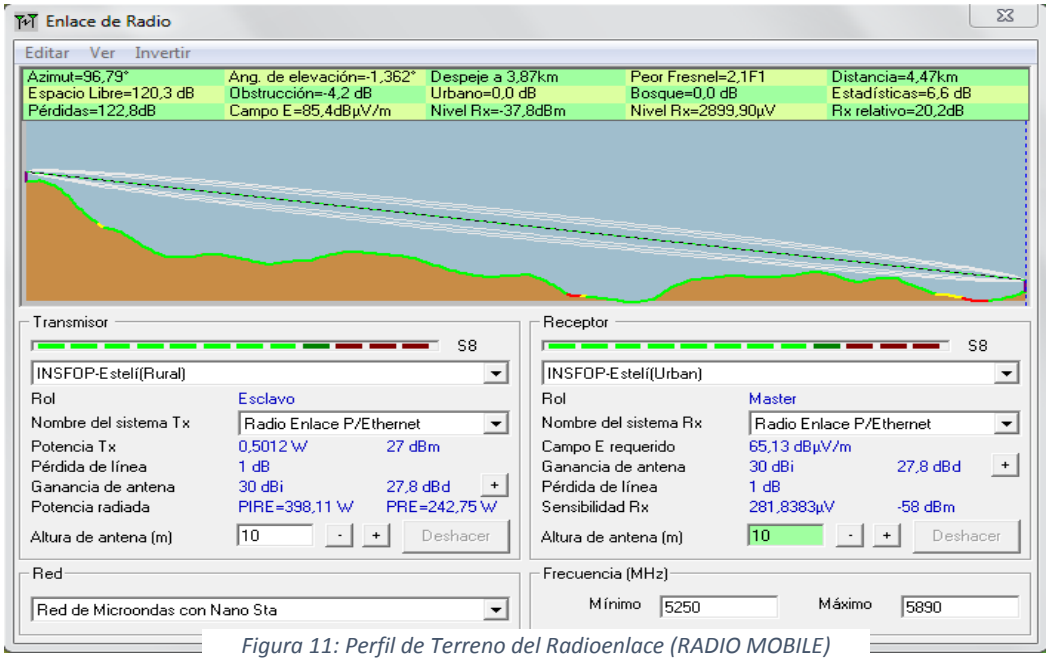


Figura 11: Perfil de Terreno del Radioenlace (RADIO MOBILE)

En la figura anterior se puede observar que la línea de visión está dibujada con una línea recta, y las diferentes variaciones de altura en el terreno(vano), a fin de evitar pérdidas por difracción se asumen a las inevitables perdidas de espacio libre , además se observa que el camino está despejado para la primera zona de Fresnel , en la que se concentra la mayor cantidad de potencia de la señal que será transmitida, cabe mencionar que cada valor obtenido en el diseño del sistema va a variar a dependencia de la frecuencia de operación elegida, los equipos utilizados , la distancia de los emplazamientos ,etc.

2.3.3- ANÁLISIS DE REFLEXIÓN

Es importante clasificar el vano en el que se hará el diseño ya que cada terreno (campos de cultivos, bosques con mucha o poca vegetación, colinas, llanos, cuerpos de agua, entre otros) posee diferentes coeficientes de reflexión que dependen a su vez de la frecuencia de operación, y como se mencionó anteriormente, la reflexión reduce la calidad de la señal debido a la cancelación que producen los desfases en el tiempo entre la señal directa y la señal reflejada.

El análisis de reflexión se hace para determinar si el enlace requiere de un sistema de protección que le permita poder operar de manera eficiente contrarrestando la reflexión, un ejemplo de un sistema protegido es la diversidad de espacio entre dos antenas receptoras separadas verticalmente, donde una separación optima entre antenas debería proporcionar un máximo en el nivel de la señal recibida en la segunda antena, cuando la antena principal se encuentra en un mínimo, y viceversa; Otro ejemplo puede ser utilizar la polarización vertical, que especialmente a bajas frecuencias ofrece una reflexión reducida, en nuestro diseño se hace uso de polarización horizontal y se obtuvieron resultados que no afectan a nuestra señal de interés. En la figura 12 se muestra un diagrama por proyección de rayos, solamente se usa para fines gráficos, debido a que las reflexiones tiene mayor incidencia en el enlace cuando pasan por cuerpos de agua o tierra plana.. (Ingvar Henne & Per Thorvaldsen, 2002)

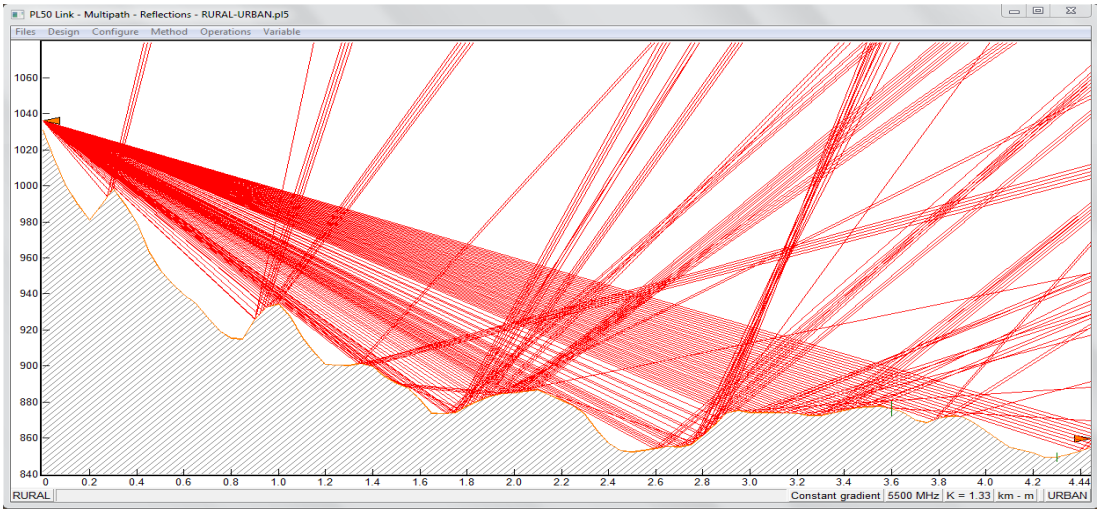


Figura 12: Análisis de Reflexión (PATHLOSS)

2.3.4- ESTANDARES Y OBJETIVOS DE CALIDAD Y DISPONIBILIDAD

Este apartado se incluye antes de discutir en detalle el radio enlace ya que no es posible diseñar un enlace sin tener en cuenta los objetivos del diseño. Conseguir que una señal de radio se reciba en un punto distante no es difícil, de hecho, las señales de interferencia indeseables pueden ser recibidas desde cientos de Kilómetros de distancia bajo ciertas condiciones de propagación. La ciencia e ingeniería en el diseño de enlaces de radio va hacia las predicciones de calidad que pueden ser esperadas para un determinado diseño de enlace.

Es muy difícil lograr que un enlace de Microondas opere al 100% libre de errores, usualmente se acude a estándares proporcionados por la ITU (UNION INTERNACIONAL DE TELECOMUNICACIONES) para guiarse, los cuales aportan ciertos criterios para ciertos circuitos típicos de conexión (rutas hipotéticas de referencia)que pueden luego ser aplicados en una conexión real; Es por esto que se necesita saber con qué tipo de sistema se está tratando y que calidad amerita, para poder aplicar atinadamente esta serie de estándares y así lograr un equilibrio disponibilidad –calidad.

La ITU divide las interrupciones en aquellas que exceden los 10 segundos y aquellas que no, para interrupciones prolongadas, donde el sistema se cae por más de 10 seg, el circuito es considerado como no disponible. Los estándares de no disponibilidad propuestos por la ITU limitan la cantidad de tiempo por año que el circuito puede caerse.

Esto incluye periodos en los cuales la taza de error de bits (BER) es peor que 10^{-3} y periodos en los cuales el enlace es desconectado.

Para interrupciones cortas, menores que 10 seg, el sistema es definido como disponible (aunque no es utilizable para el usuario durante este periodo), los estándares de rendimiento son definidos. Esto limita la cantidad de tiempo por mes que estas interrupciones cortas pueden ocurrir. (Ingvar Henne & Per Thorvaldsen, 2002)

Los principales objetivos de rendimiento y disponibilidad de la ITU están basados en las recomendaciones G.821 y G.826, las cuales son una serie de normativas y consejos prácticos para el diseñador de enlaces de microondas, como se mencionó anteriormente ,un aspecto clave y muy importante para el diseñador del radio enlaces, a la hora de escoger un estándar para aplicar, es considerar el tipo de servicio que será proporcionado y que calidad del servicio alternativo frente al cual se comparará el nuevo servicio, por ejemplo, La recomendación G.821 es inadecuada para servicios de datos de alta capacidad, a diferencia de la recomendación G.826 donde la mayoría de los sistemas prácticos funcionan en sistemas tipo E1, E3 y STM – 1.

Los objetivos de la ITU – T especificados en estándares tales como G.821 y G.826 están especificados para conexiones internacionales sobre un circuito de referencia de 27,500 Km. Es clara la importancia para el diseñador de la red que planifica una ruta de enlace de radio de unos pocos cientos de kilómetros conocer el estándar de diseño de tal manera que si dicho enlace forma parte de un circuito internacional, la conexión total cumple los objetivos. Si el circuito no forma parte de tal larga conexión internacional, puede asumirse que los objetivos son los de una red pequeña. Mientras uno se ajuste a lo especificado por el estándar ITU, técnicamente hablando, la reducida calidad que debería obtenerse podría ser mucho peor que las disponibles en otros sistemas de transmisión similares, especialmente si se emplea fibra óptica. El actual estándar usado en la práctica es un compromiso entre la convergencia de objetivos razonablemente prorrateados y alcanzar el nivel de calidad usando radio-enlaces, que sea comparado a

otras opciones de medios de transmisión que el usuario de la red podría tener.

2.3.4.1- ESTÁNDARES DE NO DISPONIBILIDAD

La no disponibilidad tiene un especial significado en los estándares de la ITU. De acuerdo a ITU – R, el período de tiempo de no disponibilidad empieza cuando, al menos una dirección de transmisión, una o ambas de las siguientes condiciones ocurre por 10 segundos consecutivos: o la señal digital es interrumpida (pérdida de alineamiento o sincronización) o el BER en cada segundo es peor que $1x10^{-3}$. Estos 10 segundos son considerados parte del tiempo no disponible.

2.3.4.2- CAUSAS DE NO DISPONIBILIDAD.

Las causas de las interrupciones largas pueden ser usualmente consideradas en tres categorías; propagación, falla en el equipo y otros.

PROPAGACIÓN

Las interrupciones relacionadas a las propagaciones, mayores que 10 segundos, son debidas principalmente a tres causas:

1.- Pérdida por Difracción:
2.- Entubamiento (Ducting):
3.- Lluvia:

PÉRDIDA POR DIFRACCIÓN

La duración de la mayoría de interrupciones por desvanecimientos por multitrayecto son menores que 10 s, uno de los desafíos reales de ingeniería de un enlace de radio están en predecir la cantidad de desvanecimiento por multitrayecto que puede ocurrir; Por consiguiente, se consideran bajo los estándares de rendimiento. Los efectos de desvanecimientos atmosféricos dominantes, los cuales afectan la disponibilidad, son debidos a la difracción de la señal de radio. Si esta pérdida causa que la señal recibida sea atenuada a un nivel tal que ya no se pueda demodular la señal, ocurrirá una interrupción. En la práctica, escogiendo las reglas de claridad adecuadas, las antenas pueden ser instaladas en alturas convenientes para que estas pérdidas puedan ser ignoradas además de otras técnicas más avanzadas

tales como la ecualización adaptiva son ahora empleadas en equipos de radio para corregir estos efectos.

ENTUBAMIENTO (DUCTING)

El Ducting es una condición que puede ocurrir si la curvatura del haz de radio excede la curvatura de la tierra, o también cuando en el vano se genera una condensación de las moléculas de agua (ducto troposférico), formando una cortina refleja la señal a diferentes direcciones; Bajo esta condición ocurren desvanecimientos con interrupciones totales de señal que pueden durar varias horas. En la práctica, esta condición puede ser usualmente ignorada desde el punto de vista de la interrupción. Las áreas geográficas que presentan un alto riesgo de falla por “ducting” están bien documentadas. Cuando esta condición existe, puede usarse, diversidad de espacio con grandes antenas para reducir su efecto.

LLUVIA

La interrupción de la propagación debido a la lluvia es proporcional a la tasa de lluvia de la región. Es importante darse cuenta de que no depende del promedio de lluvia; Es la cantidad instantánea de agua en el trayecto la que es relevante. Las moléculas de agua absorben la energía de las microondas en forma de calor, el mismo principio usado para calentar alimentos en un horno microondas.

La atenuación por lluvia causa desvanecimiento plano porque atenúa la señal recibida. La única forma para mejorar la disponibilidad es incrementar la ganancia del sistema empleando, por ejemplo, grandes antenas. Las técnicas de diversidad (frecuencia o espacio) no proporcionan mejoras, a veces ambos canales se atenúan igualmente. La diversidad de polarización proporciona una pequeña pero significativa mejora con la polarización vertical. La razón de esto es que las gotas de lluvia tienden a caer como gotas aplanadas; así la atenuación en la polarización horizontal es mayor que en la polarización vertical.

FALLA EN EQUIPO

Las interrupciones largas pueden ocurrir si fallan los equipos de radio. La no disponibilidad del enlace es la diferencia entre la disponibilidad y el 100% .Estos cálculos muestran que para aplicaciones de alta calidad los equipos deberían estar protegidos (con respaldo), sin errores de conmutación (hitless), sin embargo no es esencial dado que con cortos tiempos de "intercambio", los efectos en la interrupción total son despreciables.

OTROS

Esta categoría incluye tales eventos como el apagado para mantenimiento planificado, falla en las fuentes de poder primarias, y fallas "catastróficas" tales como incendios en la sala de equipos o la caída de la torre. La única forma de asegurar que este tipo de fallas no ocasione demasiadas interrupciones es tener alguna forma de diversificar la ruta en la red.

Otro mecanismo de interrupción que es a menudo inadvertido es el viento. Si la torre no es lo suficientemente fuerte o no está bien sujeta, oscilará por el viento, como el ancho del haz de la antena es a menudo solo la fracción de un grado, pueden ocurrir interrupciones.

La disponibilidad de un radioenlace está en relación entre los efectos de la propagación y las averías del equipo. Se presenta la disponibilidad de los módulos del equipo radio por medio del MTBF (Tiempo Medio Entre Averías). La experiencia práctica demuestra que la disponibilidad del sistema total a menudo está limitada por otros factores distintos al equipo radio en sí mismo. La indisponibilidad debido a problemas del mantenimiento, averías de energía, etc. a menudo puede ser la principal causa de la indisponibilidad del sistema, sobre todo en áreas rurales. (Ingvar Henne & Per Thorvaldsen, 2002).

CAPÍTULO III

3.1- RADIOENLACE PUNTO A PUNTO

En este apartado se describe la planificación e ingeniería de un tramo de la red que va unido por un radioenlace con visibilidad directa, en el cual se describirá de forma general un estudio de viabilidad de este sistema, con el propósito de asegurar que el radioenlace que unirá las dos sucursales cumpla con los estándares de calidad y disponibilidad. Dentro de los principales parámetros que se abarca en la planificación de esta propuesta están: la configuración de la red, la capacidad del sistema, los objetivos de la ejecución, la selección de sitios, ubicación de torres, entre otros.

En la parte más detallada de la planificación se cubren los parámetros de vano, como alturas de las antenas, tipos de antena y tamaños, condiciones geográficas y climáticas; Deben ser evaluados el funcionamiento e indisponibilidad debido a los efectos de la propagación, precipitaciones, problemas de interferencias y averías de los equipos, para lo cual se usa el software profesional PATHLOSS 5 que brinda parámetros aproximados a la realidad de la disponibilidad de nuestro enlace y los software RADIO MOBILE Y GOOGLE EARTH **,** para consideraciones gráficas.

Para culminar se realizará un presupuesto que contendrá los costos de equipos que se utilizaran en la instalación de este sistema, buscando una solución económica que cumpla con nuestros objetivos y teniendo presente la expansión futura de los servicios.

3.1.1- REPLANTEO DE CAMPO

Durante la fase de planificación del sistema de microondas se llevó a cabo un replanteo de campo, el objetivo de:

- Verificar la localización exacta de los emplazamientos.
- Verificar la línea de visión.
- Clasificar el vano.
- Comprobar las condiciones de la propagación.
- Comprobar las condiciones de la estructura donde irán montadas las torres.

Para ello se inició nuevamente con un estudio detallado del mapa digital que proporciona el software PATHLOSS 5, y la herramienta Google Earth, donde se localizó la ubicación aproximada de los emplazamientos incluyendo localizaciones alternativas, se dió una altura preliminar a las antenas, algo muy importante ya que los equipos que se eligieron para el radio enlace requieren una visión directa para una buena operación.

Se clasificó el vano como un terreno Montañoso (altitud > 700 msnm) , como también las condiciones atmosféricas, y se llegó a la conclusión que los emplazamientos serian situados en los techos de las sucursales con el fin de ahorrarse de ubicar más tramos de torres desde el nivel del suelo que además tendrían que montarse sobre bases sólidas lo que implicaría a más gasto, eligiendo montar 20 pies de tramos de torres equivalentes a 6,1 mts en cada emplazamiento que será perfectamente soportado por las estructuras de las sucursales. (Ingvar Henne & Per Thorvaldsen, 2002)

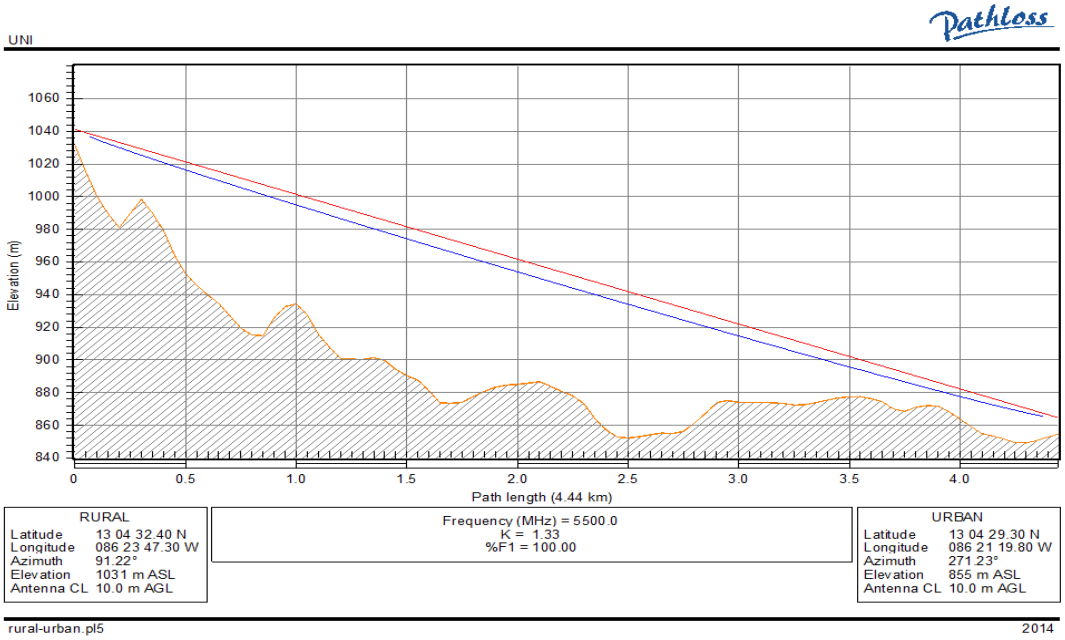


Figura 13: Replanteo de Perfil del Terreno

3.1.2- PROPUESTA

Este apartado se creó con el fin de proporcionar la documentación técnica de los equipos y accesorios que se eligieron para el diseño, la elección se lleva a cabo apegándonos a las normas y recomendaciones de la ITU-R y la ITU-T para garantizar una disponibilidad del 99.999% anual del enlace; Los suministros incluyen: antenas, equipos de radio, líneas de transmisión con sus respectivos conectores, fuente de energía, torres y accesorios para el montaje de equipos; La elección de los equipos se hizo de acuerdo a la solicitud de la institución, logrando un punto de equilibrio entre los precios y el desempeño; se da el enfoque en proponer un sistema flexible y modular a nivel de software y hardware de tal manera, que sea posible escalar a mayor capacidad de transporte cuándo INSFOP lo requiera.

Se utilizaran los acrónimos URBAN y RURAL para hacer referencia a las sucursales de la institución INSFOP ubicados en la parte rural y urbana de la ciudad de Estelí respectivamente, los equipo que a continuación se describirán son válidos para ambos sitios. Para mayor información, refiérase al manual de operación específico de los equipos propuestos, que se pueden conseguir navegando por internet.

3.1.2.1- EQUIPOS DE RADIO

Para la propuesta se requirió de una tecnología de radio con matriz IP pura, capaz de manejar paquetes, con funcionalidad de emulación de E1, y manejo de protocolos de sincronismo; Las características que se tomaron en cuenta para la elección fueron: proveer la capacidad de usar Ethernet como una capa común de transmisión para transportar y discriminar los diferentes tipos de tráfico transportado sobre el flujo Ethernet.

El ROCKET M5 – UBIQUITI (SITIO- URBAN y SITIO - RURAL) Es un radio resistente, de alta potencia, con un buen funcionamiento en la gama de los 50km a más, opera a velocidades de transmisión de 150+Mbps reales bajo el protocolo TCP / IP. Provee una excelente calidad en servicios de voz, dato y video, es un equipo diseñado específicamente para al aire libre, utilizado para aplicaciones en enlaces punto a punto (PP) y punto a multipunto (PTMP), otra característica es que se puede administrar mediante una interfaz web que facilita su manejo, por medio de la cual se pueden variar

los parámetros del enlace para obtener una mejor calidad, y cuenta con diferentes aplicaciones, una de ellas es un analizador de espectro, que le permite al operador identificar posibles fuentes de interferencia.

Estos equipos operan con el protocolo de Acceso Múltiple por División de Tiempo (TDMA), lo que le permite a cada usuario enviar y recibir datos en diferentes intervalos de tiempo "Time Slot", eliminando colisiones y maximizando la eficacia de tiempo en antena, lo que proporciona muchas mejoras de funcionamiento en la latencia, el rendimiento, y la adaptabilidad comparada a todos otros sistemas exteriores en su clase.

3.1.2.2- LÍNEA DE TRANSMISIÓN

El cable blindado CAT 5e, para este caso, se necesitara un Shielded twisted pair o STP (en español "par trenzado blindado"); El STP un producto de alta calidad para aplicación en exteriores, cuenta con 4 pares de alambre torcido 24 AWG con blindaje de cinta de aluminio de 0.35um y alambre de drenado ESD (Carga Electrostática) para prevenir ataques y daño por ESD. El diseño multicapa de los cables les permite soportar las más duras condiciones climáticas y uso rudo. Excelente para uso en aplicaciones de red en exteriores, transferencias de datos e incluso líneas telefónicas. Ofrece soporte a velocidades 10/100 Mbps. Este tipo de cables pueden usarse en dos niveles:

Level1- Cable Blindado Categoría 5e para exteriores tipo Carrier-Class.

Level2- Cable Blindado Categoría 5e para exteriores con divisor "anti-crosstalk" blindaje adicional y está probado para proveer óptimo desempeño en redes Ethernet Gigabit.

Nota: Se necesitaran 100 pies (aproximadamente 30.5 mts) para cada extremo del enlace.

3.1.2.3- CONECTORES

Los conectores blindados RJ-45 Ubiquiti son recomendados para este tipo de conexiones, y adecuados para el tipo de cable (STP CAT 5e), que gracias a sus características, hacen que cuando se cierra el circuito sea menos

sensible al ruido y radiaciones, a la vez que le sirve de protección a los equipos.

Para un máximo rendimiento de los conectores se recomienda usar cubiertas protectoras, para prevenir filtraciones de agua.

Nota: Se necesitaran al menos de 4 a 6 conectores para cada extremo del enlace.

3.1.2.4- ANTENAS

En el diseño del radio enlace se propone el uso antenas de plato Ubiquiti 802.11a/n High Power AirMax MIMO TDMA UB-ROCKETDISH-5G-30; es un tipo de antena altamente direccional, que han sido desarrollados para operar junto con el Rocket M5 de modo transparente. No es necesaria ninguna herramienta especial para montar el Rocket M5 en la antena Rocket Dish, simplemente se desliza en el montaje específicamente diseñado para este propósito.

La UB-ROCKETDISH-5G-30 es una antena de plato de 5 GHz doble polaridad de la serie AirMax, ha sido diseñada instantáneamente para la serie UB-ROCKETM5 para crear poderosos MIMO 2 x 2, su uso para exteriores y enlaces punto a punto, tiene un precio económico, un buen rendimiento, el montaje Rocket está diseñado a prueba de mal tiempo.

Figura 14: Antenas Rocket Dish 5GHz 30dB y Equipos de Radio Rocket M5

3.1.2.7- TORRES, ACCESORIOS Y DEMÁS MATERIALES.

Como se mencionó anteriormente, se recomienda la instalación de dos tramos de torre de 8 pulgadas de ancho por 10 pies de largo, para cada sitio, que sumados con la altura de las sucursales, lse lograría un aproximado de 10 mts, los necesarios para un buen funcionamiento según el diseño; Se optó por este método para reducir costos, ya que de esta manera se evita la instalación de más tramos a nivel del suelo que serían necesarios para conseguir una altura estimada, lo que traería consigo más gastos en tramos, bases de concreto y demás materiales.

A continuación se detallan los accesorios y materiales necesarios para la instalación:

30 lbs de cable galvanizado nº 12, se utilizara para los vientos de la torre.

6 Tensores de ½ pulgada.

½ galón de impermeabilizado.

1 bolsa de bridas plásticas para sujetar el cable UTP a la estructura de la torre.

Etc.

3.1.3- REPORTES DE RESULTADOS OBTENIDOS EN EL DISEÑO.

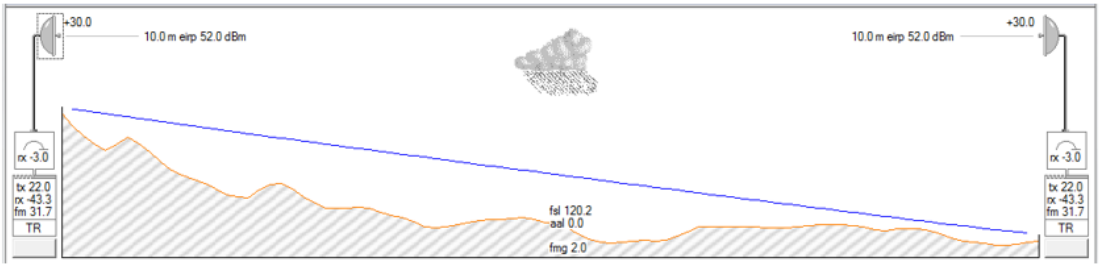
En este apartado se busca evidenciar que los sistemas ofertados cumplen o mejoren los criterios de calidad normalizados, para lo cual se presenta un reporte de ingeniería que se obtiene una vez hecho todos los cálculos y consideraciones; Este reporte fue generado por la herramienta de diseño para sistemas de Microondas PahtLoss 5, en el cual se introducen los datos técnicos de los equipos recomendados, con el objetivo de verificar si cumplen con una Disponibilidad del 99.999% anual.

Es importante el uso de un software para el cálculo disponibilidad de estos sistemas, por esto, una vez elegidos los sitios probables de instalación, siempre es aconsejable hacer un cálculo de presupuesto de potencia con las antenas y equipos propuestos. De esta manera el instalador llegará al sitio con un nivel de señal teórico el cual debe de concordar dentro de un margen de seguridad con el nivel recibido. Si este nivel no se alcanza dentro de +-5dBs se puede concluir que existe algún problema que se pasó por alto y debe de solucionarse antes de proceder a la entrega del servicio.

Los resultados son presentados en la siguiente tabla donde se muestra un conjunto de datos obtenidos con el software, que una vez realizado los respectivos cálculos, se puede apreciar que se tiene un sistema con buenos parámetros de disponibilidad, lo que ayuda a tener una visión del comportamiento de los equipos en la red, y a tomar decisiones bastante acertadas a la hora de llevar a cabo el proyecto.

UNIVERSIDAD NACIONAL DE INGENIERIA

Pathloss



	RURAL	URBAN
Latitude	13 04 32.40 N	13 04 29.30 N
Longitude	086 23 47.30 W	086 21 19.80 W
True azimuth (°)	91.22	271.23
Elevation (m)	1031.11	854.69
Tower type	roof mount	roof mount
Antenna model	RD-5G-30 (TR)	RD-5G-30 (TR)
Antenna code	rd-5g30	rd-5g30
Antenna gain (dBi)	30.00	30.00
Antenna diameter (m)	0.65	0.65
Antenna height (m)	10.00	10.00
TX line model	STP CAT 5e	STP CAT 5e
TX line length (m)	25.00	25.00
TX loss (dB)	0.00	0.00
RX loss (dB)	3.00	3.00
Frequency (MHz)	5500.00	
Polarization	Horizontal	
Path length (km)	4.45	
Free space loss (dB)	120.24	
Atmospheric absorption loss (dB)	0.04	
Field margin (dB)	2.00	
Net path loss (dB)	65.27	65.27
Radio model	ROCKET M5	ROCKET M5
TX power (watts)	0.16	0.16
TX power (dBm)	22.00	22.00
EIRP (dBm)	52.00	52.00
RX threshold level (dBm)	-75.00	-75.00
Receive signal (dBm)	-43.27	-43.27
Thermal fade margin (dB)	31.73	31.73
Worst month multipath availability (%)	99.99992	99.99992
Worst month multipath unavailability (sec)	2.05	2.05
Annual multipath availability (%)	99.99997	99.99997
Annual multipath unavailability (sec)	8.92	8.92
Annual 2 way multipath availability (%)	99.99994	
Annual 2 way multipath unavailability (sec)	17.84	
Rain region	ITU Region P	
Rain rate (mm/hr)	724.48	
Flat fade margin - rain (dB)	31.73	
Rain attenuation (dB)	31.71	
Annual rain availability (%)	100.00000	
Annual rain unavailability (min)	0.00	
Annual rain + multipath availability (%)	99.99994	
Annual rain + multipath unavailability (min)	0.30	

Figura 15: Parámetros de Disponibilidad

3.2- DISEÑO DE LA VPN

3.2.1- INSTALACION

Se utilza el sistema operativo Windows para demostrar el funcionamiento de la VPN ya que es el más utilizado, se descarga el software en la página oficial de OpenVPN https://openvpn.net/index.php/open-source/downloads.html y se procede a instalarlo con permisos de administrador. Durante la instalación es necesario marcar los componentes que por defecto están desactivados, estos corresponden a OpenSSL Utilities ya OpenVPN RSA Certificate Management Scripts, ya que se necesitarán para crear las llaves para la encriptación y cifrado de nuestros datos.

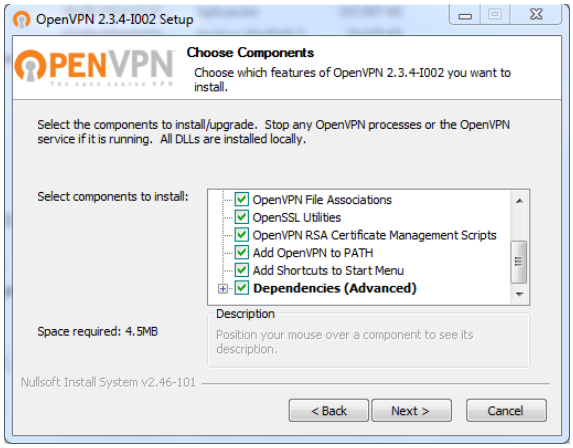


Figura 16: Componentes de OpenVPN a Instalar

Seguidamente aparece una alerta de que se instalara un adaptador de red, y que posiblemente el controlador de dicho adaptador no está firmado, a pesar de esto, es muy importante instalar el adaptador debido a que se manipulará para nuestra VPN.

OpenVPN creará una entrada al registro con la extensión de archivos **.ovpn** los cuales son archivos de configuración que tienen las pautas necesarias para poder realizar la conexión VPN.

Lo siguiente es hacer que el servicio se inicie junto con el sistema operativo para garantizar, ante cualquier situación, perdidas mínimas en la conexión, para ello se dirige a Panel de Control – Herramientas Administrativas – Servicios y se busca el servicio de OpenVPN.

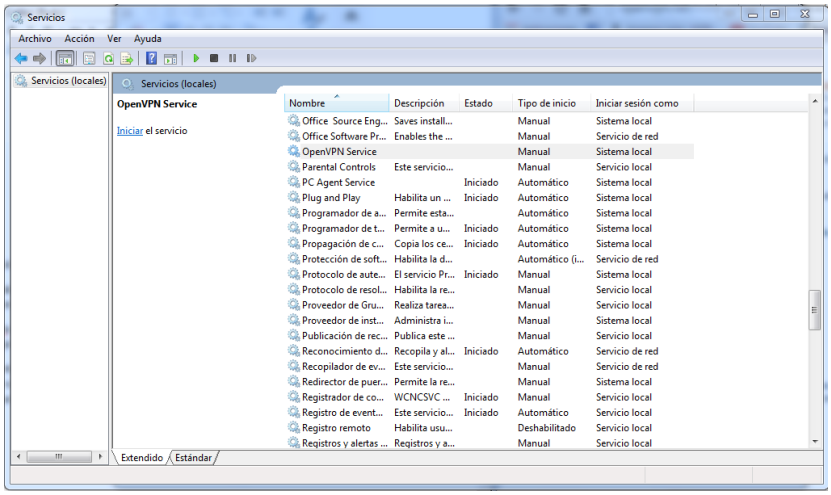


Figura 17: Inicio Automático del Servicio

Se hace Clic derecho en él – Propiedades y se procede a cambiar el tipo de inicio de Manual a Automático, para que el servicio siempre se ejecute como administrador, se hace clic secundario sobre el acceso directo de OpenVPN, en la pestaña de compatibilidad se marca la casilla “ejecutar como administrador”.

3.2.2- VPN ENRUTADA O PUENTEADA?

OpenVPN ofrece 2 tipos de conexiones VPN, la enrutada (Routed) y la que usa conexión de puente (Bridged), generalmente la enrutada es la mejor opción para la mayoría de los casos debido a que es más fácil de configurar y tiene controles de acceso selectivos dependiendo del cliente conectado, sin embargo la puenteada está orientada para implementar servicios específicos como aplicaciones que se basan en difusiones de broadcast ya que esta variación de VPN trata a los clientes como si estuvieran en la misma LAN del servidor facilitando muchísimo la implementación de los servicios de voz, siendo así, convergente con el servidor PBX y el radioenlace, también es amigable en cuanto a datos en general, opcionalmente puede trabajar con un servicio DHCP para asignar direcciones IP dentro la LAN del servidor. Ya que se propone servicios de voz y datos en general, el tener lógicamente la red como si fuese una sola LAN facilita muchas cosas, es por esto que se optó por la variante puenteada de OpenVPN.

3.2.3- CONEXIÓN DE PUENTE

Ya que se eligió la variante Puenteada, se debe crear una conexión de puente, para esto se dirige al panel de control, en el apartado de Centro de redes y recursos compartido, se busca la opción de cambiar configuración de adaptador, ahí se encontrarán nuestros adaptadores de red incluyendo el anteriormente instalado, el cual se puede indentificar a través del nombre de fabricante (TAP-Windows Adapter), para crear el puente solo selecciona nuestra interfaz Ethernet y al mismo tiempo nuestra interfaz TAP, cuando ambas estén seleccionadas se procede a hacer clic derecho, seguidamente se selecciona Conexiones de puente y automáticamente se creara otra interfaz la cual es el puente entre nuestra interfaz física y la interfaz virtual de nuestra VPN.

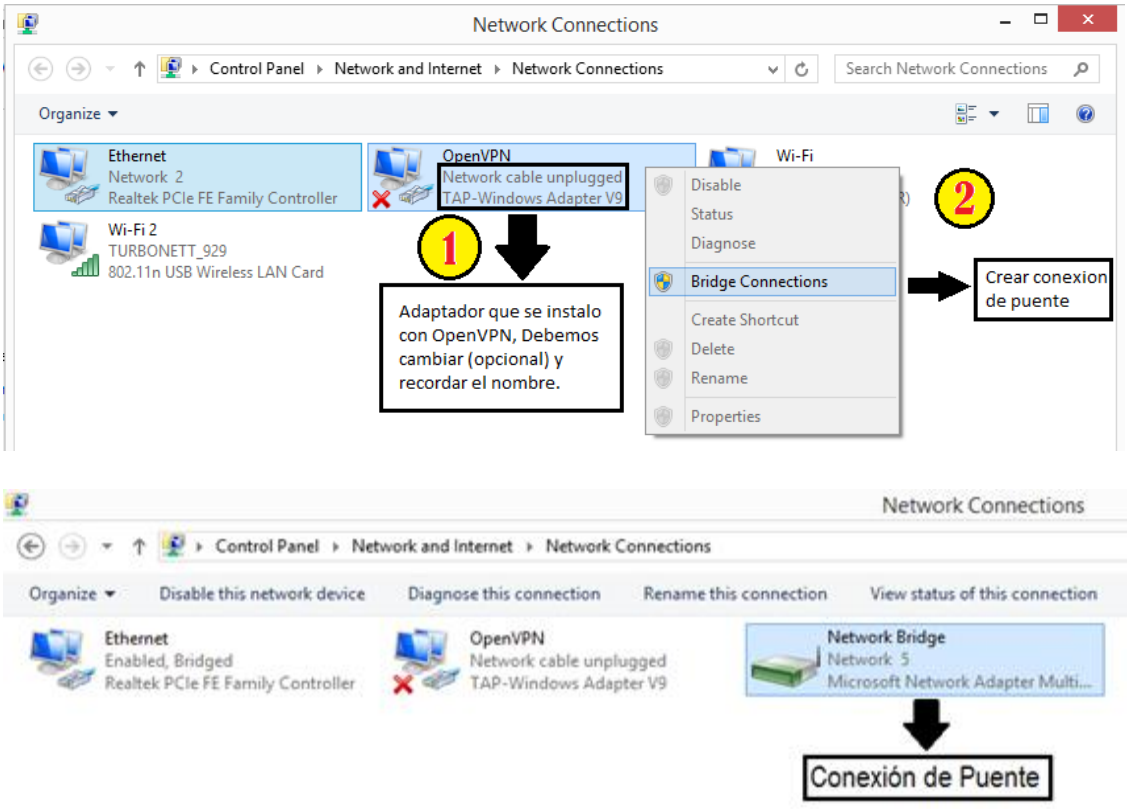


Figura 18: Conexión de Puente

Nota: Esto se debe hacer tanto para el servidor como para el/los cliente(s).

3.2.4- CERTIFICADOS Y LLAVES

Antes de establecer una configuración de OpenVPN es necesario construir un PKI (Public Key Infrastructure) el cual consiste en una serie de certificados y llaves tanto públicas como privadas que utilizaran nuestros dispositivos en la conexión VPN. Posteriormente se explica cómo generar los elementos que conforman la PKI:

3.2.4.1- CERTIFICADO DE AUTORIDAD MAESTRO Y SU LLAVE.

Para generar el CA y su correspondiente llave se utilizan un conjunto de scripts RSA (Rivest, Shamir, Adleman) que es un algoritmo criptográfico de llave pública, estos archivos vienen incluidos en la instalación del software, se pueden encontrar en la carpeta de instalación de OpenVpn "**C:\Archivos de programa\OpenVpn\easy-rsa**" antes de iniciar se debe saber explorar desde el CMD de Windows hacia la carpeta "**easy-rsa**" todo se debe hacer como administrador.

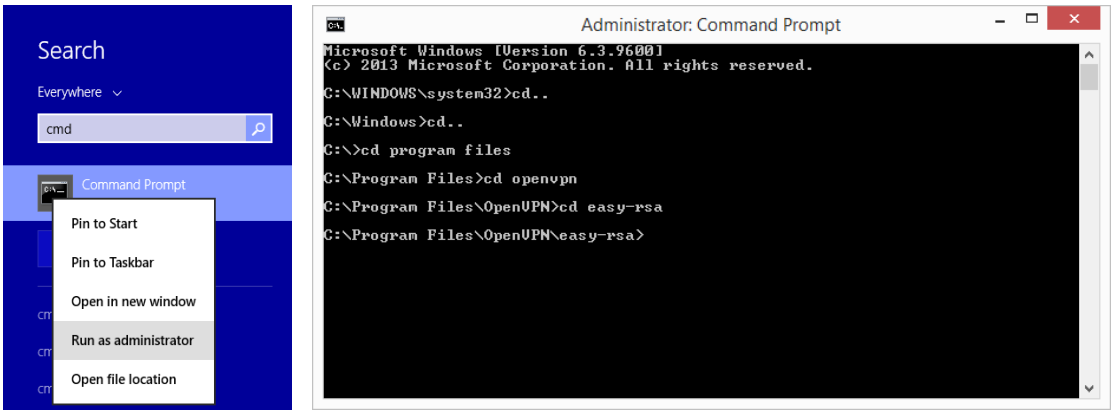


Figura 19: Directorio easy-rsa

Con el comando "**cd..**" se sube un directorio y con el comando "**cd carpeta**" se ingresa a un directorio llamado **carpeta**, en nuestro caso el sistema operativo está en ingles por lo cual varia el nombre de "Program Files",

Antes de proseguir se debe saber con qué archivos se va a trabajar, dentro de la carpeta **easy-rsa** están varios ficheros, el más importante es **vars.bat.sample** el cual es una base, se renombra a **vars.bat**, este archivo

contiene los parámetros que se usaran para generar los certificados, las llaves públicas y privadas.

Para generar el Certificado de Autoridad Maestro CA se edita el archivo **vars.bat**, se abre con un editor de textos, se recomienda abrir el bloc de notas como administrador y desde el mismo, abrir el archivo, se recuerda que para editar archivos de instalación se necesitan privilegios de administrador, de lo contrario no permitirá guardar los cambios que se le hagan al archivo. Como referencia se tiene el archivo por defecto con la explicación de cada parámetro:

```
set KEY_COUNTRY=US              ## Pais
set KEY_PROVINCE=CA             ## Departamento
set KEY_CITY=SanFrancisco       ##Municipio
set KEY_ORG=OpenVPN             ##Nombre de Organizacion
set KEY_EMAIL=mail@x.com        ## Correo de Organizacion
set KEY_CN=changeme             ## Debe ser cambiado por cada certificado
set KEY_NAME=changeme           ## Nombre cualquiera opcional cambiarlo
set KEY_OU=changeme             ## Nombre cualquiera opcional cambiarlo
```

Los demás parámetros pueden quedar por defecto.

Nota: el archivo **vars.bat** debe editarse por cada certificado y llave que se genera, siendo la variable más importante a cambiar el COMMON NAME (KEY_CN), no se puede generar otro certificado a base de un **vars** que ya se utilizó.

Más Información (Ingles): http://openmaniak.com/openvpn_pki.php

Una vez dentro de ese directorio y editado el **vars** se procede a usar los binarios para crear el Certificado de Autoridad CA, se colocan los comandos en nuestra ventana de terminal (CMD) en el siguiente orden

Vars # Se carga el archivo vars.bat en memoria.

Clean-all # Mueve los parámetros de vars cargados en memoria a un directorio conocido

Build-ca # Genera el Certificado de Autoridad Maestro CA y su llave a partir de vars.bat

Nota: Puede que aparezca una advertencia de OpenSSL, se puede hacer caso omiso porque el script de igual manera genera los archivos que se necesitan usando configuraciones que se instalaron junto a OpenVPN usando un cifrado de 1024bits, esto es válido para todos los certificados y llaves que se generarán.

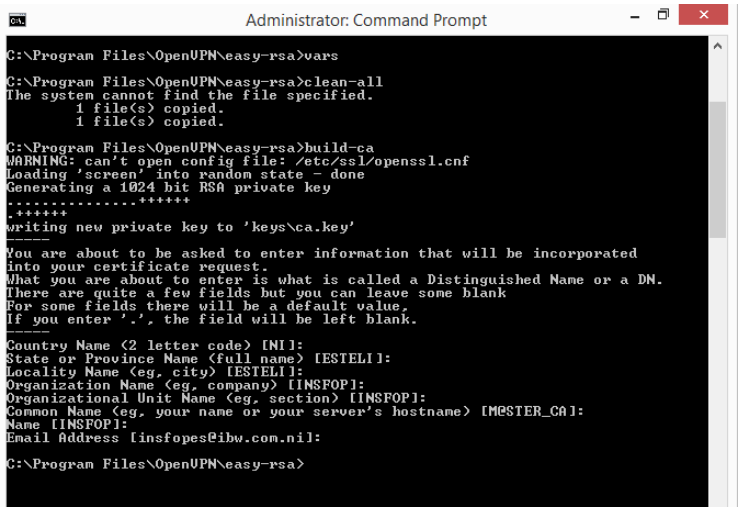


Figura 20: Creando Certificado Maestro

3.2.4.2 CERTIFICADO Y LLAVE DEL SERVIDOR VPN

Seguidamente se genera el certificado y llave del servidor, nuevamente se debe editar el archivo vars.bat con los datos que corresponden a la empresa/lugar donde se encuentre el servidor, una vez hecho se carga en el CMD usando el comando "**vars**" , se prosigue tecleando el comando "**build-key-server NOMBRE**" donde **NOMBRE** será el nombre del servidor, este dato es meramente referencial.

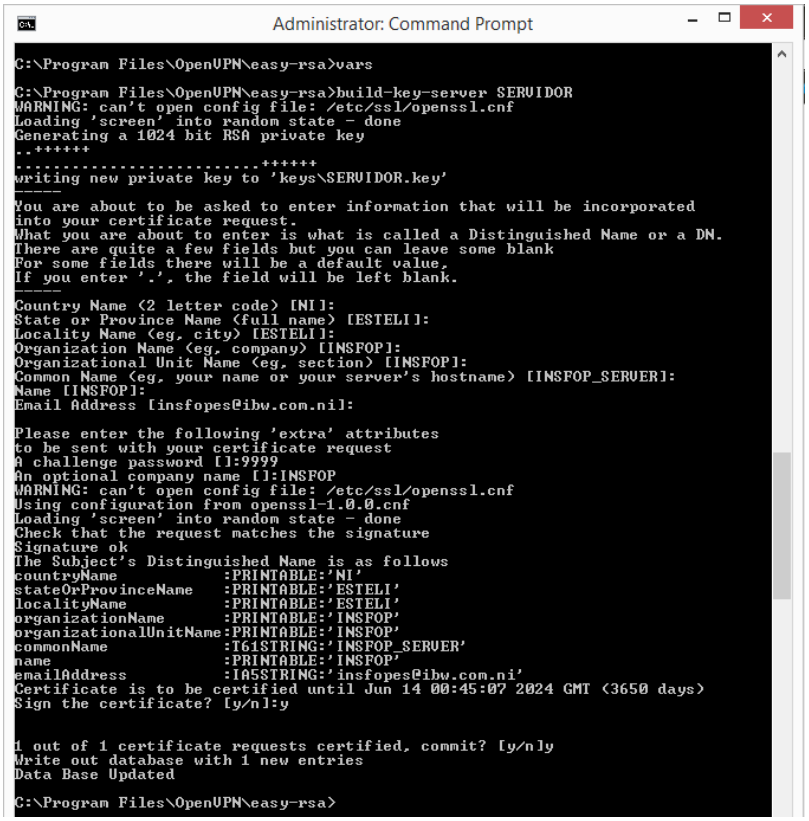


Figura 21: Creando Llave y Certificado del Servidor

La contraseña de reto (Challenge Password) puede ser cualquiera, se debe guardarla por cuestiones de seguridad y respaldo, las preguntas que hace deben responderlas con un "y" seguido de la pulsación de la tecla ENTER

Hasta el momento se ha creado el Certificado de Autoridad con su llave, y el Certificado del servidor con su llave, resta el certificado del cliente que se conecta al servidor.

3.2.4.3 CERTIFICADO Y LLAVE DE CLIENTE

De nuevo se cambian los valores de vars.bat, esta vez para que se adecuen a los datos y lugar del cliente. Se repite el paso anterior cambiando el comando "**build-key-server NOMBRE**" por "**build-key NOMBRE**"

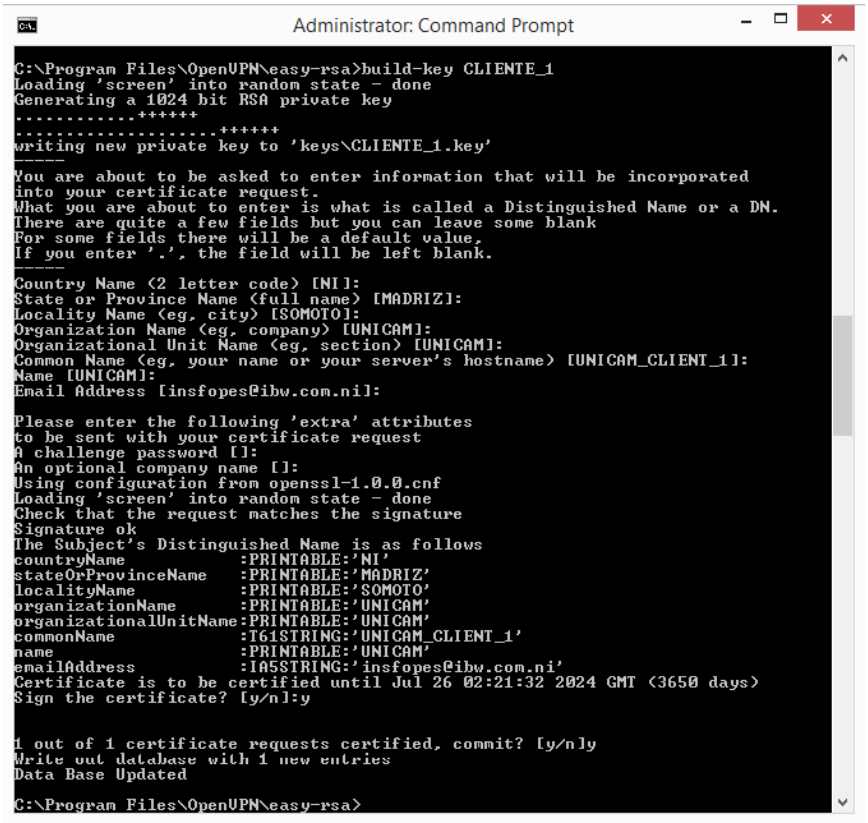


Figura 22: Creando Certificado y Llavo de Cliente(s)

Nota: Se debe repetir este último paso para cuantos clientes se pretendan tener.

3.2.4.4 PARÁMETROS DE DIFFIE HELLMAN

El protocolo criptográfico Diffie-Hellman es un protocolo de establecimiento de llaves entre partes que no han ten ido contacto, se utilizará para implementarlo en el servidor. Para generar estos parámetros solo se necesita ejecutar el comando "**build-dh**"

Figura 23: Creando Parámetros Diffie-Hellman

Ahora que ya se tienen generado todos los certificados y llaves necesarios, se pueden encontrar dentro de la carpeta **keys** dentro del directorio **easy-rsa**.

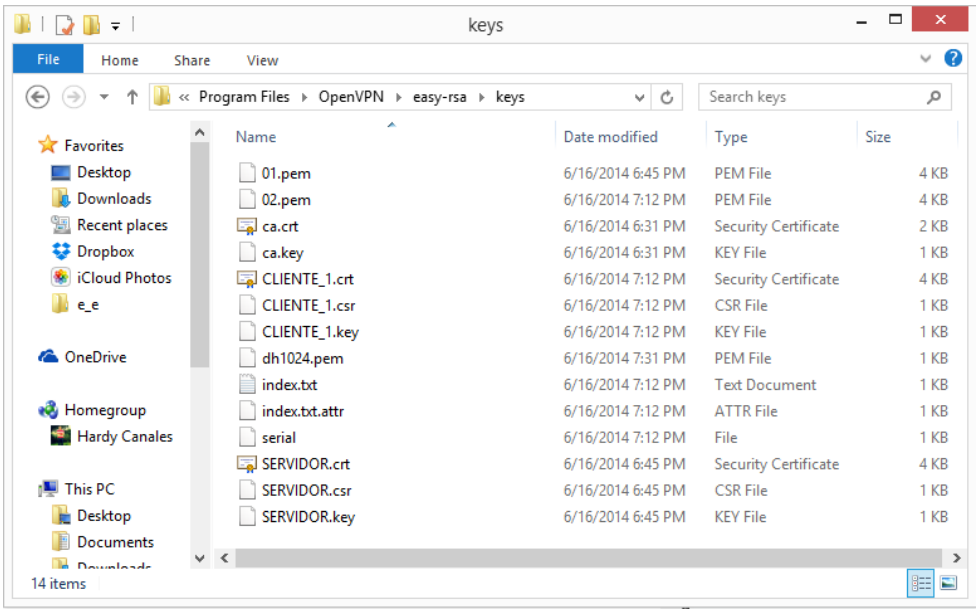


Figura 24: Archivos Creados Con los Scripts

Para una mejor comprensión, se explican los archivos más relevantes que se generaron en la siguiente tabla:

Archivo	Dispositivo Correspondiente	Explicación	Secreto
ca.crt	Servidor y todos los clientes	Certificado de Autoridad Raíz	No
ca.key	Solo la maquina firmadora de llaves	Llave Raíz o Maestra (CA)	Si
Dh1024.pem	Servidor	Parámetros DH	No
SERVIDOR.crt	Servidor	Certificado del Servidor	No
SERVIDOR.key	Servidor	Llave del Servidor	Si
CLIENTE_1.crt	Cliente 1	Certificado de Cliente 1	No
CLIENTE_1.key	Cliente 1	Llave de Cliente 1	Si

3.2.5- PERFILES DE OPENVPN

Los perfiles son archivos de configuración de texto que contienen las configuraciones e instrucciones que tendrá el servidor, las líneas comentadas es decir las que comienzan con un "**#**" explican la función de cada directiva (en inglés), si un comando tiene un "**;**" al inicio de su línea significa que éste está desactivado, para activarlo solamente se debe remover el "**;**".

Perfil del Servidor:

Antes de continuar se debe copiar los archivos correspondientes al servidor (ver tabla anterior) en la carpeta "**config**".

Dentro del directorio de instalación, específicamente dentro de la carpeta "**sample-config**" se pueden encontrar muestras de perfiles que se tomaran como base para crear las nuestras, para ello se debe, nuevamente abrir el bloc de notas con permisos de administrador y se prosigue a editar el archivo que corresponde al servidor "**server.ovpn**" siguiendo las recomendaciones a continuación:

- Como se está trabajando con VPN puenteada (Bridged) se debe utilizar **server-bridge** y **dev tap** y comentar las líneas de **server 10.8.0.1 255.255.255.0** y **dev tun** (que solo usan en la variante enrutada).
- Si se desea que el servidor VPN escuche puertos TCP en lugar de UDP se usa **proto tcp** en lugar de **proto udp** (*recomendado udp*).
- Cuando se instaló OpenVPN se instaló un adaptador de red virtual, para que el servicio reconozca el adaptador que debe usar, se debe activar la línea "**dev-node MyTap**" donde **MyTap** es el nombre que tiene el adaptador virtual, en nuestro caso se renombra a "**OpenVPN**".
- El puerto oficial por defecto de OpenVPN asignado por IANA es el puerto 1194, se recomienda liberar el puerto en la configuración de los enrutadores o firewalls para que el tráfico pueda salir sin impedimento alguno, de lo contrario no se podrá establecer la conexión entre servidor y cliente.

- En la parte donde se define el directorio de los archivos de certificados y llaves anteriormente creados, se debe usar el siguiente formato para indicar en el perfil donde se encuentran tales archivos, es decir doble pleca invertida y entre comillas dobles por ejemplo resultaría así:

  ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"

  cert "C:\\Program Files\\OpenVPN\\config\\SERVIDOR.crt"

  key "C:\\Program Files\\OpenVPN\\config\\SERVIDOR.key"

  Se hace lo mismo para el archivo del protocolo criptográfico Diffie–Hellman:

  dh "C:\\Program Files\\OpenVPN\\config\\dh1024.pem"
- Se tienen 2 directivas que contienen "**server-bridge**" la primer sintaxis es [IP Local del Servidor] [Mascara de subred] [Primer IP a asignar a los clientes] [Última IP a asignar a los clientes] (ejemplo: **server-bridge 192.168.1.2 255.255.255.0 192.168.1.100 192.168.1.200**). La segunda directiva solo contiene "**server-bridge**" que es para activar el servidor para que contenga servicios DHCP y pueda asignar el rango IP definido anteriormente a la interfaz puente del cliente.
- Por último se activa el parámetro "**client-to-client**" para que, en un dado caso que hallan varios clientes conectados al servidor, todos ellos se puedan percibir entre sí.

Perfil del Cliente:

De manera similar al servidor se copian los archivos correspondientes al cliente en la carpeta **"config"**, esta vez se emplea el perfil **client.ovpn** como base para configurar la parte del cliente,

- Se activa la línea **"dev tun''** para indicar al cliente que es una VPN puenteada, y a su vez se desactiva la línea "**dev tap"**.
- Se quita el punto y coma de la línea **dev-node MyTap**, donde, **MyTap** es el nombre del adaptador de red virtual del **cliente,** dicho nombre puede diferir del nombre del adaptador del servidor, hay que recordar que el nombre del adaptador en el perfil debe coincidir

con el nombre del adaptador TAP para que el software esté al corriente de cual adaptador de red va a manipular, en nuestro caso se renombra el adaptador TAP del cliente a OpenVPN_Cliente y así mismo debe configurado en el perfil del cliente.

- En la directiva **“remote my-server-1 1194” , my-server** es la IP publica que el ISP asigne a la red donde se encuentra el servidor, para esto se debe hacer uso de un sitio web que identifique nuestra IP , como por ejemplo www.cualesmiip.com:

Figura 25: IP Pública

El puerto **1194** es el que se utiliza, por lo tanto solo es necesario cambiar **my-server** por la IP pública.

La mayoría de los proveedores de internet asignan esta dirección IP de forma dinámica lo que significa que cada cierto tiempo se tendrá que estar modificando esta información en el perfil del cliente cada vez que no se pueda establecer la conexión. Para evitar esto se recomienta contratar un servicio que incluya una IP pública única con algún proveedor de internet del país, o bien un DDNS (servicio de DNS Dinámico,hay un par de servicios DDNS gratis por la web como www.noip.com), el cual asignará un nombre de dominio que automáticamente “apunta” a la dirección pública que se tenga aunque ésta cambie aleatoriamente cada cierto tiempo. El servicio de DNS Dinámico se encarga de mantener en concordancia la IP pública que se posea con el nombre de dominio que asigne, además se deberá configurar la

redirección de puertos (Port Forwarding) en el router que sirva de Gateway al servidor, para que las peticiones de los protocolos sean redirigidas al servidor, el puerto UDP 1194 (Puerto oficial de OpenVPN), debe ser redirigido a la IP que tenga en el servidor o al nombre de host en caso de tener servicio DNS Dinámico, esta última configuración se hace en la interfaz de configuración del router Gateway del servidor.

Del mismo modo que en el servido,r se editan las direcciones de los archivos pero esta vez en la parte del cliente:

ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config\\CLIENTE_1.crt"
key "C:\\Program Files\\OpenVPN\\config\\ CLIENTE_1.key"

Hay que hacer mención que estos archivos van en la maquina cliente, los demás parámetros en el perfil los se dejan por defecto.

3.2.5- CONEXIÓN ENTRE SERVIDOR Y CLIENTE

Hasta este punto se debe tener todo en orden para hacer la conexión entre cliente y servidor, en el servidor se hace clic derecho sobre el icono correspondiente a OpenVPN en la barra de tareas se busca el nombre que tenga nuestro perfil ovpn y se selecciona connect, si existe algún error se puede ver el archivo de registro para ver que puede estar ocasionando algún problema, para ello se hace click en **View Log**

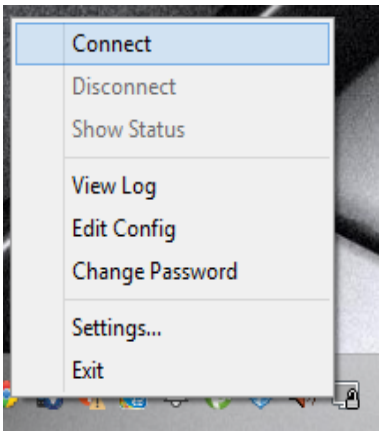


Figura 26: Ejecutando el Servicio en el Servidor

Se mostrará una ventana registro (log), al ser primera vez que se ejecuta el servicio saltara un mensaje del firewall, el cual consulta si se quiere dar permiso a OpenVPN para conectarse a las redes, se dejan seleccionadas ambas opciones (redes públicas y redes privadas) y se le da clic a permitir acceso.

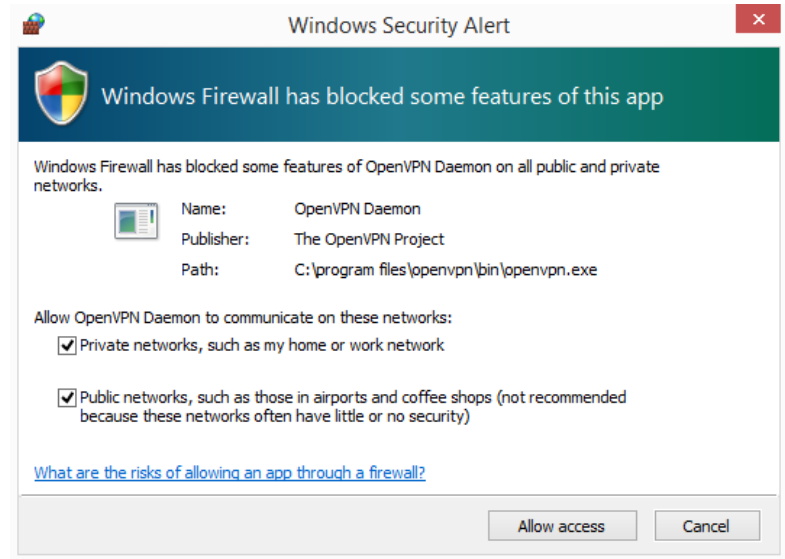


Figura 27: Proporcionando Permisos al Servicio

Seguidamente el icono de OpenVPN se pondrá de color verde y se mostrara en estado **conectado.**

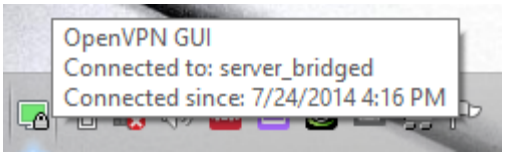


Figura 28: Servicio Ejecutándose

CLIENTE

En el lado del cliente se debe tener dentro del directorio "**config**" 3 archivos que son, **ca.crt, CLIENTE_1.crt y CLIENTE_1.key,** además de estos, también el perfil **client.ovpn** que se modificó anteriormente, luego de copiar cada archivo donde corresponde (Máquina cliente) se abre OpenVPN (siempre con permisos de administrador), clic secundario, luego clic a **connect.** Si todo está en orden se conectará al servidor satisfactoriamente y se asignara un IP dentro del rango que se configuró en el perfil:

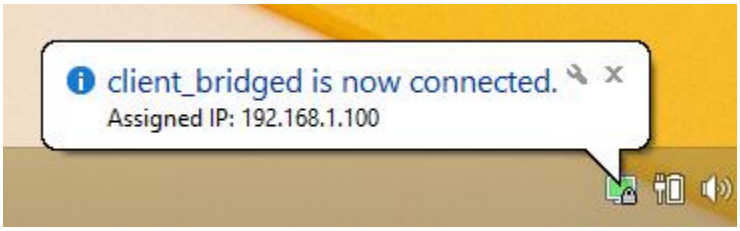


Figura 29: Cliente Conectado al Servidor VPN

Se puede observar que se asignó la dirección IP **192.168.1.100**, se configuró el DHCP del segmento de red del servidor para asignar direcciones IP desde **192.168.1.10** hasta **192.168.1.99**, todos los clientes tendrán direcciones IP desde **192.168.1.100** hasta **192.168.1.200**, Ambos segmentos de red (segmento del cliente y segmento del servidor) ahora están lógicamente distribuidos como si de una sola LAN se tratase.

Nota: Existe una discrepancia con la dirección IP de la interfaz puente, con la dirección IP que asigna el servidor, en este caso se debe configurar una IP estática en el puente cliente que sea la que el servidor asignó.

3.3- SERVIDOR PBX (Asterisk)

Para el diseño del entorno telefónico se propone utilizar la distribución gratuita de Linux AsteriskNOW instalada de manera virtual (usando el software libre gratis VirtualBox) en la misma computadora que el servidor VPN, para ello la computadora deberá tener 2 puertos/tarjetas Ethernet, uno por cada servicio (PBX y VPN).

Se descarga la imagen binaria de la distribución marcada como **estable** de http://asterisk.org/downloads/asterisknow se copia la imagen en un disco o se hace booteable desde una usb y se procede a arrancar el sistema operativo desde Asterisk.

1. Una vez en la pantalla de instalación se presiona la tecla ENTER aparecerá la siguiente pantalla:

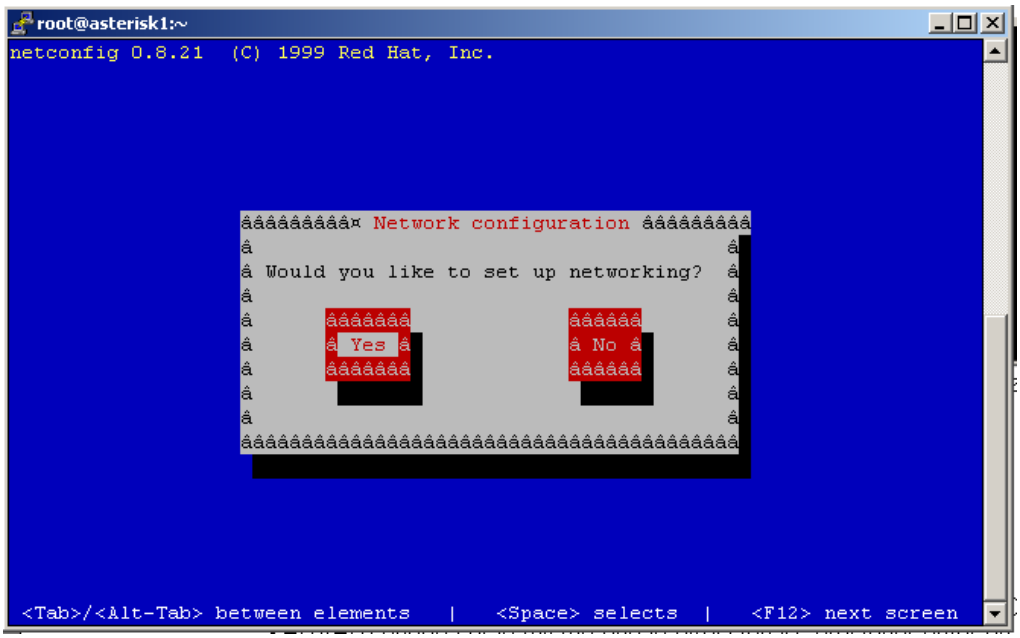


Figura 30: Pantalla de Inicio de Instalación de Asterisk

Se debe dar ENTER en la opción YES.

2. A continuación aparecerá una pantalla de configuración, en la cual se debe configurar la dirección de IP del servidor.(**dirección asignada según criterios del administrador de la red**).

   Ej.: 10.2.33.214. La dirección IP debe estar en el mismo segmento de red que el router y de todas las computadoras que van a utilizar el software de teléfono voIP

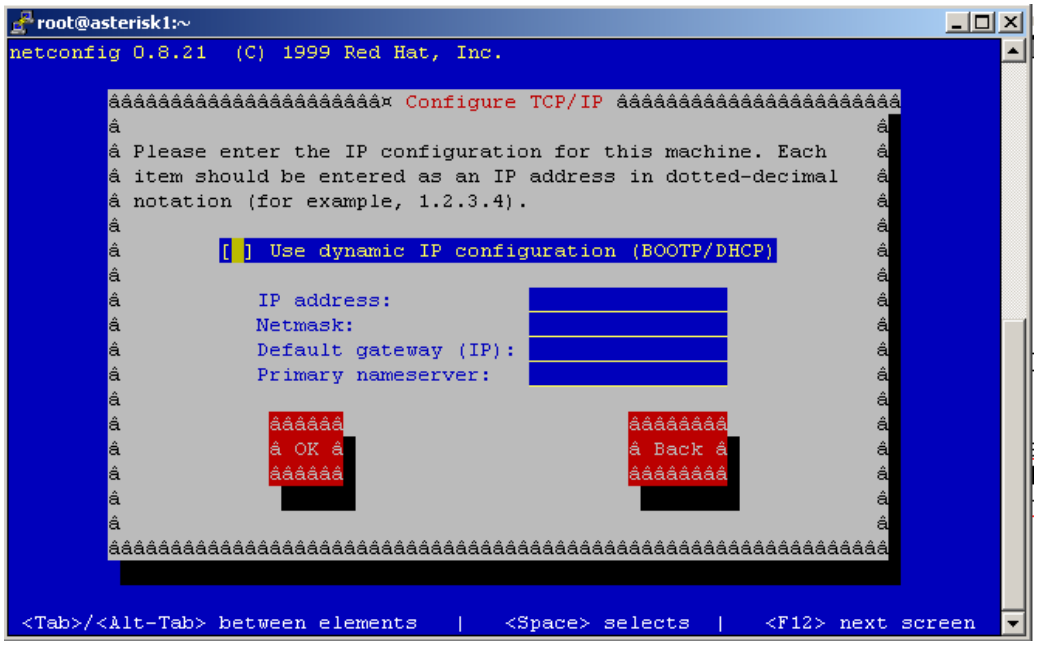


Figura 31: Configuración de Parámetros de Red del Servidor Asterisk

3. Seguidamente introducir la máscara de red (Netmask), la dirección IP del Gateway y una dirección de servidor DNS para la resolución de nombres. (**Todos estos parámetros también a conveniencia y selección del administrador de la red**), presionar ENTER en OK y se mostrará la pantalla de comando.

4. Una vez instalado el Servidor de Asterisk es necesario cambiar o establecer nuevas cuentas de usuario y contraseñas del servidor. Se comienza por establecer una cuenta de usuario y contraseña de la interfaz Web de Asterisk, para hacerlo, se escribe en la línea de comando la dirección IP que se le asignó al servidor en el punto 3 (por ejemplo: **10.2.33.214**).

Durante la instalación el software debió haber solicitado ingresar un nombre de usuario y contraseña, esos mismos datos se deben ingresar para acceder a la interfaz gráfica del servidor. .

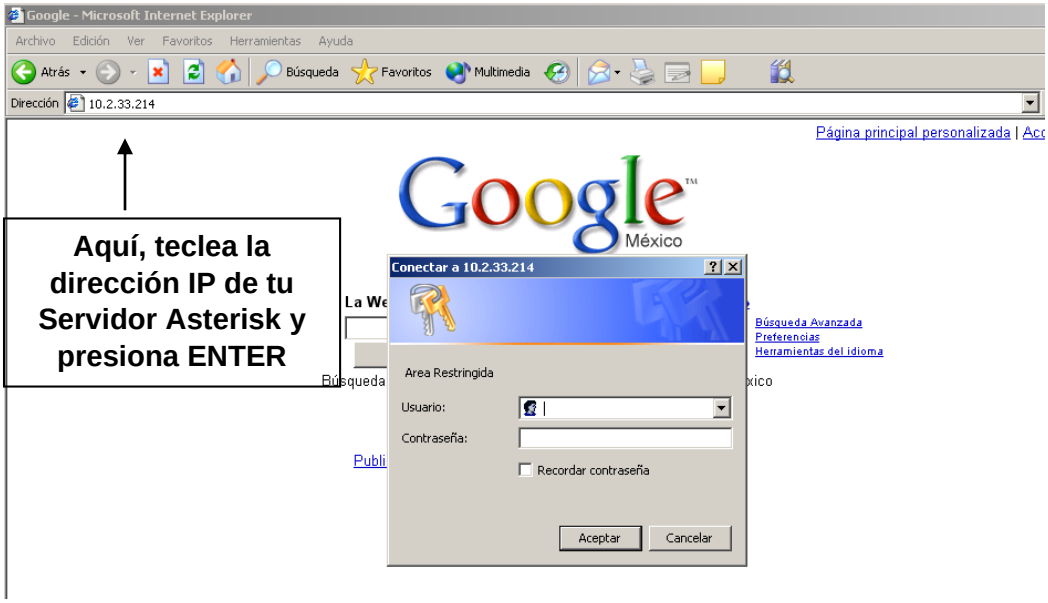


Figura 32: Ingresando a la GUI del Servidor

Una vez ingresado los datos se procede a hacer clic en aceptar para entrar a la página del servidor Asterisk, se dirige a la pestaña **Extensions** y a continuación se debe llenar el siguiente formato como se indica a continuación (JKsistemas, 2014):

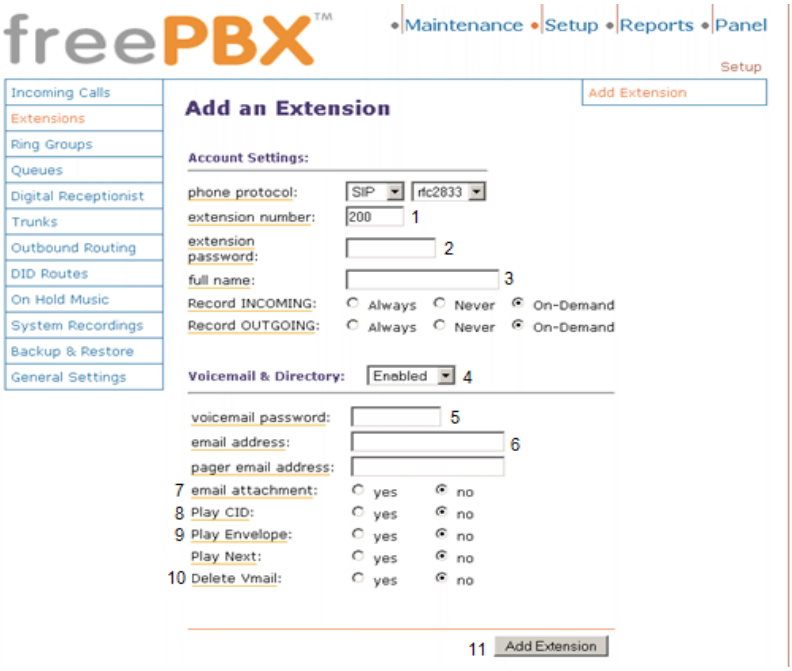


Figura 33: Parámetros de Extensiones de Asterisk

1. Teclear número de la extensión
2. Ingresar una contraseña para la extensión
3. Suministrar el nombre del usuario de la extensión
4. Habilitar correo de voz (ENABLED)
5. Ingresar una contraseña para el buzón de voz de la extensión
6. Ingresar la dirección de correo electrónico en la cual deseas que se mande una copia del mensaje de voz.
7. Habilitar a YES Email Attachment si deseas recibir una copia de los mensajes de tu correo de voz
8. Play CID: esta opción es para incluir en el mensaje la extensión del emisor y la hora en que fue mandado
9. Play Envelope: esta opción es para agregarle al mensaje de voz la fecha y hora del mensaje.
10. Delete Vmail: si activas esta opción (yes) el mensaje se borrará del buzón de voz después de haber sido reenviado a tu cuenta de correo
11. Presiona con el Mouse en **Add** Extensión cuando hayas terminado para agregar la extensión, después presionar la barra roja que aparece en parte superior de la pantalla para actualizar cambios (refresh) (JKsistemas, 2014).

3.4- SOFTPHONE

Usando el software ZOIPER s puede hacer y recibir llamadas aplicando las configuraciones pertinentes de las extensiones creadas por cada usuario en el softphone. Cada computadora en cada entidad o sitio de la institución, deberá tener una extensión y usuario registrado en el servidor Asterisk para que el software ZOIPER pueda conectarse con las credenciales de la extensión al mismo. Una vez realizado esto los usuarios podrán utilizar el software como si de un teléfono se tratase pudiendo hacer llamadas de voz a todas las demás extensiones en línea que estén registradas en el servidor.

Más información sobre configuración e instalación:

Manual versión gratis:

http://www.zoiper.com/downloads/Zoiper_2.0_Free_Manual.pdf

Guía Rápida:
http://www.zoiper.com/en/documentation/windows-installation-and-configuration

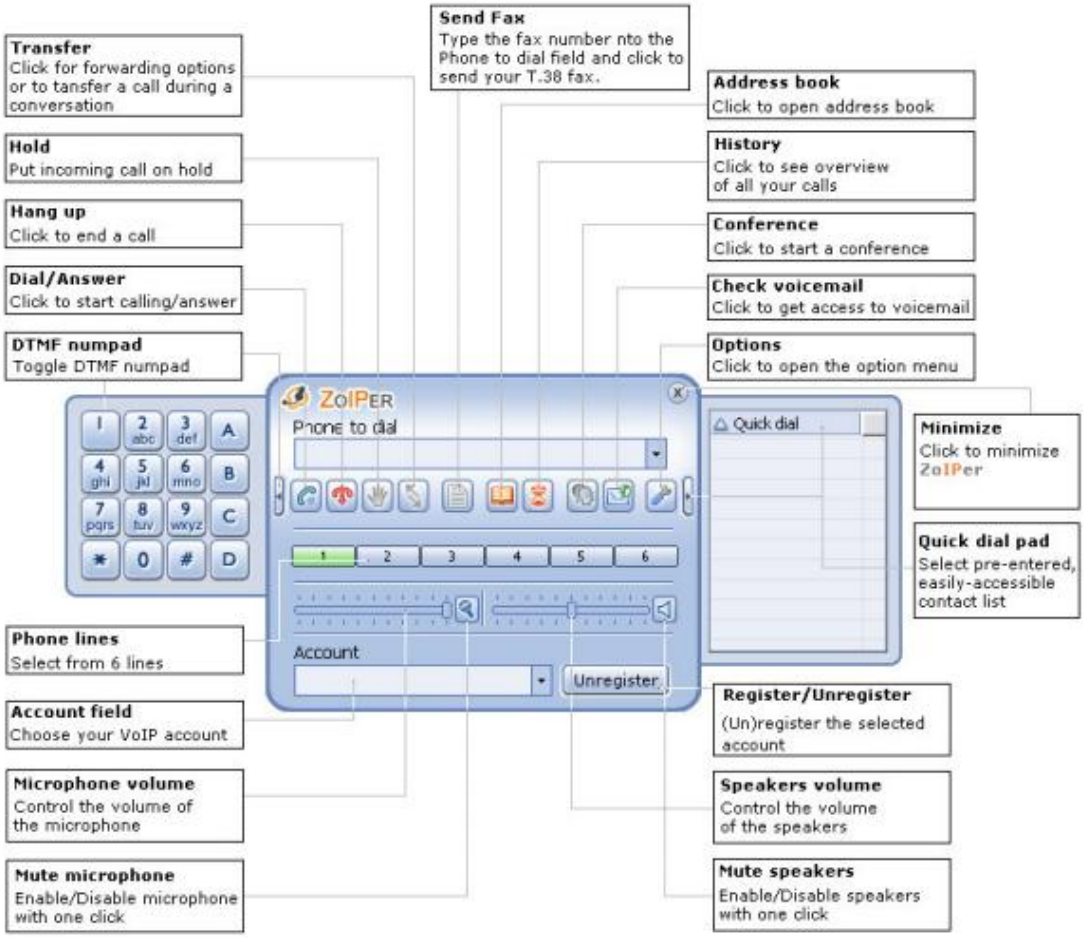


Figura 34: Pantalla de Inicio de ZOIPER

3.5- TOPOLOGÍA DE LA RED

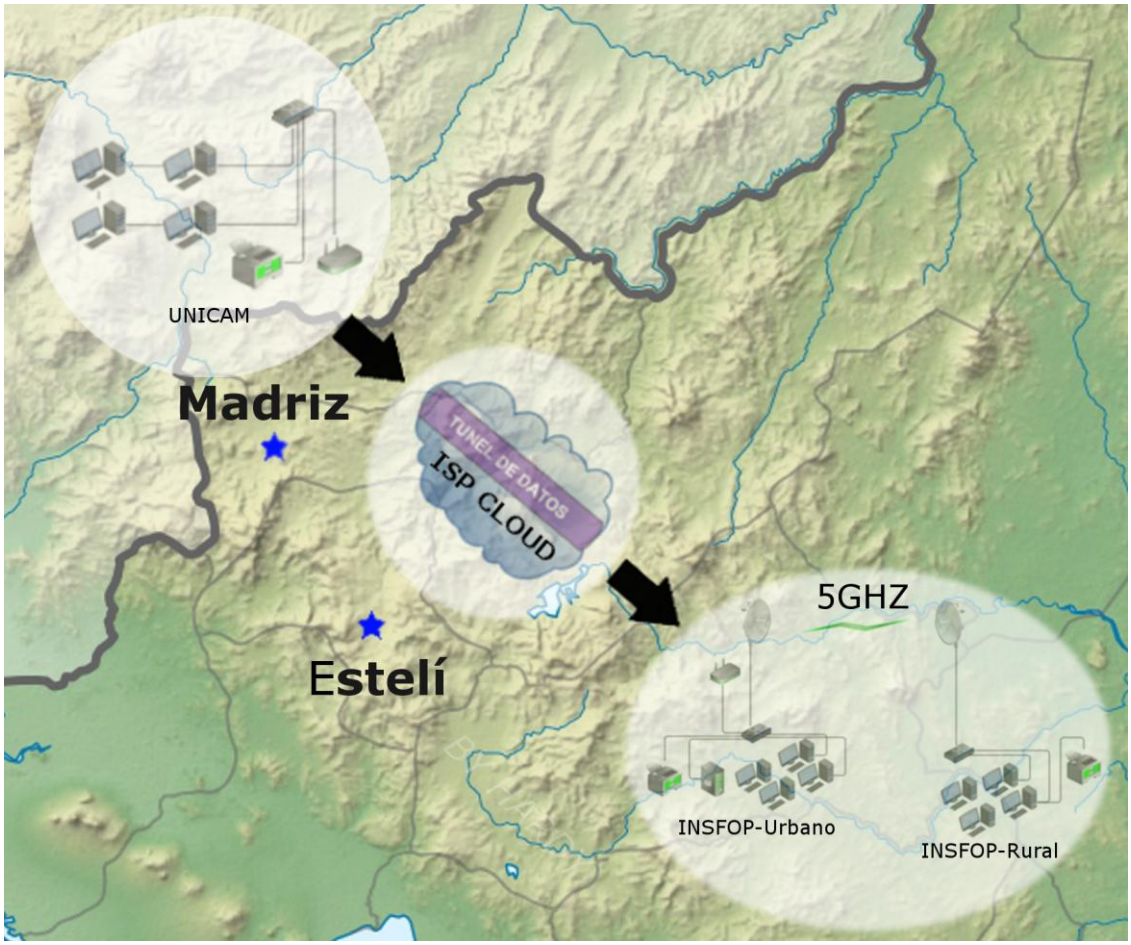


Figura 35: Topología de la Red desde el Punto de Vista Geográfico

3.6- PRESUPUESTO

El presupuesto del proyecto es de gran importancia tanto para el **Instituto de Formación Permanente "INSFOP"** , como para nosotros , ya que ha llevado a que se investiguen las soluciones más favorables y eficaces en el mercado de las telecomunicaciones en nuestro país; En esta parte se vieron involucradas diferentes empresas que impulsan el desarrollo, ofreciendo soluciones flexibles de comunicación, gestión y productividad, que ayudan al éxito de las diferentes instituciones y negocios, acelerando sus operaciones y encaminándolas en el mundo digital y de las TICs.

Las soluciones que se han elegido para esta propuesta permitirán a "**INSFOP"**, conectar sus filiales en una misma red de forma transparente al usuario final, lo que les ayudará a ahorrar tiempo, obtener información a tiempo de su institución, comunicarse en tiempo real, cara a cara y sin necesidad de viajar; Además que les permitirá controlar y monitorear el uso de sus recursos, teniendo el control de sus propias políticas de seguridad a la hora de brindarle a cada usuario por separado privilegios para el uso de sus recursos (llamadas telefónicas internas , externas , uso de internet ,entre otras) en general una alta disponibilidad, calidad y seguridad, tal propuesta se realizó pensando en futuro de manera que irá adaptándose al crecimiento de la institución de forma rápida y sencilla.

En las siguientes tablas se detallan los costos de los diferentes equipos:

PRESUPUESTO APROXIMADO PARA IMPLEMENTACIÓN DE PROYECTO

ENLACE DE MICROONDAS				
Nº	Descripción del Producto	Cantidad	Precio Unidad	Precio
1	CABLE STP CAT5E INT/EXT GRIS CMR.NEWLINK	61	C$ 20,92	C$ 1.276,12
2	CONECTOR RJ45 CAT5E/6 BLINDADO MACHO NEWLINK	12	C$ 14,64	C$ 175,68
3	PERNO C-HEXAGONAL 3/8X2 HILLMAN	16	C$ 6,22	C$ 99,52
4	TUERCA HEXAGONAL 3/8-16 HILMAN	16	C$ 1,47	C$ 23,52
5	ALAMBRE GALVANIZADO Nº 10	30	C$ 21,12	C$ 633,60
6	TENSOR OJO C/GANCHO 1/2 681KG TRUPER	12	C$ 93,93	C$ 1.127,16
7	TAPA GOTERA NEGRO SISTA 1/4	1	C$ 169,97	C$ 169,97
8	CINTA TAPA GOTERA 4"(METRO)3M_4001-0061	3	C$ 78,19	C$ 234,57
9	TAPE ELECTRICO 3/4X20MTS VINYL NEGRO SUPER	2	C$ 91,26	C$ 182,52
10	CANALETA 10X10MM CON ADHESIVO EAGLE	4	C$ 29,55	C$ 118,20
11	CINTA AMARRE 11"X4MM NEGRO 3M	50	C$ 2,09	C$ 104,50
12	ANCLAS P/SUJETAR VIENTOS	6	C$ 50,00	C$ 300,00
13	GRILLETE P/SUJETAR TENSORES	6	C$ 40,00	C$ 240,00
			Total C$:	C$ 4.685,36
			TOTAL USD	$178,35
			* Cambio	26,27

ANTENAS Y ACCESORIOS				
Nº	Descripción del Producto	Cantidad	Precio Unidad	Precio
14	ANTENA ESTACION ROCKET M5 MODEL: RD-5G-30 DIAMETRO: 0,65 mts	2	$ 450,00	$ 900,00
15	RADIO ROCKET M5 5470-5825 MHz 150+Mbps 500	1	$ 320,00	$ 320,00
16	RADIO ROCKET M5 5470-5825 MHz 150+Mbps	1	$ 320,00	$ 320,00

17	TRAMO DE TORRE DE 8"X 10 PIES	4	$ 55,00	$ 220,00
18	MANO DE OBRA DE INSTALACION	1	$ 300,00	$ 300,00
			TOTAL USD	$2.060,00
			TOTAL RADIOENLACE	$2.238,35

SERVIDOR PBX Y VPN (AMBOS EN UNA SOLA PC)				
Nº	Descripción del Producto	Cantidad	Precio Unidad	Precio
19	PROCESADOR INTEL CORE I5 4670K	1	$ 250,00	$ 250,00
20	TARJETA MADRE MSI H81-P33	1	$ 60,00	$ 60,00
21	DISCO DURO 500GB SATA WESTERN DIGITAL	1	$ 55,00	$ 55,00
22	RAM KINGSTON 4GB DDR3	1	$ 55,00	$ 55,00
23	MONITOR LED AOC 15,6"	1	$ 75,00	$ 75,00
24	CASE CPU	1	$ 45,00	$ 45,00
25	UPS FORZA LPS 750VA NT-761	1	$ 45,00	$ 45,00
26	CABLE DE PODER	2	$ 4,00	$ 8,00
27	NIC ETHERNET 2X	1	$ 18,00	$ 18,00
28	TECLADO Y MOUSE CONVENCIONALES	1	$ 15,00	$ 15,00
28	COSTOS DE VOIP	0	$ -	$ -
29	Fxo PARA ASTERISK. MARCA DIGIUM	1	$ 150,00	$ 150,00
GASTOS DE MANO DE OBRA				
30	GASTOS DE MANO DE OBRA (INSTALACION, CONFIGURACION, PRUEBAS, ETC...)	0	$ 1.500,00	$ 1.500,00
			TOTAL SERVIDOR(ES) USD	$ 776,00
			TOTAL FINAL USD	$ 3.014,35
			TOTAL FINAL C$	C$ 79.187,08

CONCLUSIONES

La tecnología de VoIP, con la utilización de los protocolos de señalización, provee comunicaciones confiables de voz con alta calidad en las transmisiones. Por tanto la propuesta planteada, es determinante para garantizar las comunicaciones entre las distintas sedes que conforman INSFOP.

La VPN propuesta constituye una sublime solución para las instituciones en cuanto a seguridad, confidencialidad e integridad de los datos, lo cual es de suma importancia en cualquier organización, todo esto sin importar la ubicación geográfica de las mismas, lo que reduce significativamente el costo de la transferencia de datos entre sedes.

La eficacia del radioenlace entre Estelí y Madriz se pudo homologar usando las herramientas computacionales previamente proyectadas, las cuales indicaron un panorama positivo para la instalación y operación del mismo en cuanto al relieve del terreno, línea de vista, propagación, atenuación, reflexiones y fiabilidad.

Se determinaron los costos del proyecto para conocer la inversión requerida para su implementación; La elección de los equipos se hizo de acuerdo a la solicitud de la institución, logrando un punto de equilibrio entre los precios y el desempeño; se hizo el enfoque en proponer un sistema flexible y modular a nivel de software y hardware de tal manera, que sea posible escalar a mayor capacidad de transporte, por ende servicios, cuándo INSFOP y UNICAM lo requieran.

La propuesta elaborada proporcionaría una red convergente, que permitirá conectar las dos sedes INSFOP en Estelí con su filial UNICAM en Madriz, y con ello, tener un sistema de comunicación moderno, seguro, económico y fiable que brindará servicio de voz, video y datos.

RECOMENDACIONES

Se recomienda el estudio de la propuesta como una base de referencia para su implementación con PYMEs, MICROPYMEs y pequeñas empresas en crecimiento, que necesiten mejorar su productividad y capacidad estratégica a través de una solución moderna y favorable.

Recomendamos que este trabajo sea agregado como un caso de estudio para fortalecer el desarrollo de habilidades en los softwares (OpenVPN, Asterisk, RadioMobile, Pathloss y programas a fines), esto con el fin de llevar la enseñanza de la mano con simuladores y consigo proporcionar una inducción más interactiva en las clases.

Sería de gran utilidad para los futuros trabajos realizar una plataforma online para que se pueda tener acceso al centro de documentación donde se almacenen los trabajos monográficos de manera digital hechos por estudiantes de la universidad.

Si se decide implantar la propuesta cabe mencionar que se necesita colocar un analizador de espectro en cada uno de los lugares donde se va instalar el enlace de radio para ver que la frecuencia en que se transmitirá no está ocupada, para su posterior inscripción en las oficinas de TELCOR, se tiene que abocar a la ventanilla única de Atención a Usuarios y Operadores, esto nos permitirá tener registrada la frecuencia de operación y proteger nuestro enlace en caso de futuras interferencias. Al estar inscrito en TELCOR aseguramos que si nuestro enlace es obstruido por otro, TELCOR tomaría medidas contra el otro usuario ya que el que inscribe primero tiene potestad sobre la banda de frecuencia usada.

Una vez Implementada la tecnología propuesta, se debe hacer un estudio de tráfico para ver si se amerita aumentar un servicio con más ancho de banda en las instalaciones de las sedes para que no exista saturación en la red y así mismo tengan un uso eficiente de la misma.

BIBLIOGRAFÍA

3CX. (12 de Febrero de 2014). Obtenido de 3CX: http://www.3cx.es/centralita-telefonica/free-edition/

(2014 de Mayo de 5). Obtenido de Centralita IP: http://www.quarea.com/es/que_es_telefonia_ip

Asterisk. (26 de Marzo de 2014). Obtenido de Asterisk: http://www.asterisk.org/

Caire, R. J. (18 de Mayo de 2014). *LUGRo.* Obtenido de Grupo de usuarios de Software Libre Rosario: http://www.lugro.org.ar/sites/default/files/introvpn.pdf

Falcón, J. A. (2007). *VoIP : la telefonía de Internet.* Paraninfo.

Golio, M. (2008). *RF AND MICROWAVE CIRCUITS,MEASUREMENTS, AND MODELING* (Second Edition ed., Vol. The RF and Microwave Handbook). (J. Golio, Ed.) Phoenix, Arizona, U.S.A: CRC PRESS Taylor & Francis Group.

Informatica Hoy. (18 de Mayo de 2014). Obtenido de http://www.informatica-hoy.com.ar/redes/Ventajas-de-las-Redes-Virtuales-Privadas.php

Ingvar Henne & Per Thorvaldsen. (2002). PLANIFICACION DE RADIOENLACES DE VISIBILIDAD DIRECTA. *Segunda edición*. Bergen: NERA -enabling a wireless future.

JKsistemas. (16 de Septiembre de 2014). *es.slideshare.net.* Obtenido de Slideshare: http://es.slideshare.net/JKsistemas/asterisk20manual

OpenVPN Technologies, I. (25 de Junio de 2014). *OpenVPN*. Obtenido de How To: https://openvpn.net/index.php/open-source/documentation/howto.html

Puma, F. A. (5 de Mayo de 2014). *Repositorio Digital EPN.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/4698/1/CD-4321.pdf

Rodríguez, A. S. (16 de Septiembre de 2014). *UPCT.* Obtenido de http://repositorio.bib.upct.es/: http://repositorio.bib.upct.es/dspace/bitstream/10317/737/1/pfm35.pdf

Soluciones con Tecnología Linux. (19 de Mayo de 2014). Obtenido de richard-davila.blogspot.com: http://richard-davila.blogspot.com/2011/04/servidores-vpn.html

VoipForo. (25 de Mayo de 2014). Obtenido de VoipForo: http://www.voipforo.com/IAX/IAXvsSIP.php

Wikipedia. (6 de Mayo de 2014). Obtenido de OpenVPN: http://es.wikipedia.org/wiki/OpenVPN